Metoder til systematisk fareidentifikation - som kan bruges i sammenhæng med risikovurderingsprocessen i CSM-RA

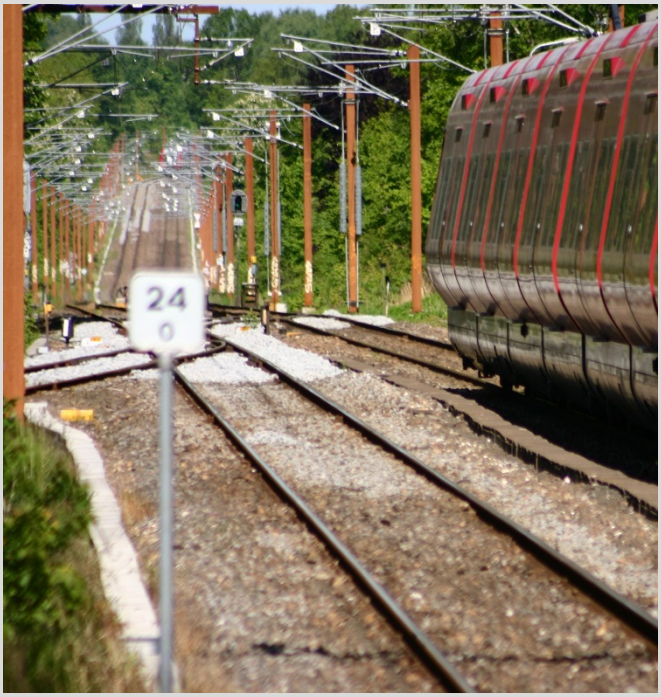
Duijm, Nijs Jan

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

Metoder til systematisk fareidentifikation

som kan bruges i sammenhæng med risikovurderingsprocessen i CSM-RA



Engineering Systems

DTU Management Engineering

Nijs Jan Duijm

December 2015

DTU Management Engineering
Department of Management Engineering

Metoder til systematisk fareidentifikation
som kan bruges i sammenhæng med risikovurderingsprocessen i CSM-RA

Rapport
2015

Af
Nijs Jan Duijm

Forsidefoto: Colorbox
Udgivet af: Institut for Planlægning, Innovation og Ledelse, Produktionstorvet, Bygning 424, 2800 Kgs. Lyngby
Rekvireres: www.man.*dtu.dk*

Forord

Denne vejledning er udarbejdet efter aftale med Trafik- og Byggestyrelsen med henblik på at hjælpe de danske jernbaneaktører når de skal udarbejde risikovurderinger i overensstemmelse med CSM-RA-forordningen (European Commission, 2013). Denne vejledning beskriver fareidentifikation som én af de elementer i risikovurderingen. I aftalen med Trafik- og Byggestyrelsen indgår også bidrag til Trafik- og Byggestyrelsens vejledninger om systemdefinition og risikoacceptprincipper.

Vejledningen er udarbejdet i samarbejde en referencegruppe. Følgende personer deltog i referencegruppen:

- Joakim Böcher — TÜV SÛD
- Daniel Orth — Atkins Danmark A/S
- Pernille Thorup Adeler — Rambøll
- Kirsten Mark Hansen — COWI A/S
- Ahmed Lütfi Øzer og Flemming V Hansen — DSB
- Claus René Pedersson — Banedanmark
- Emil Hundrup Rasmussen og Diana Rose Jørgensen — Trafik- og Byggestyrelsen

En gennemgang af teksten i forhold til CSM-RA-forordningen og anden relevant lovgivning blev gennemført af Trafik- og Byggestyrelsen.

Projektet blev styret af en styregruppe. Følgende personer deltog i styregruppen:

- Marianne Clod Zauner og Leif Funch — Trafik- og Byggestyrelsen
- Lars Nordahl Lemvigh og Claus Ingemann — DSB
- Søren Stahlfest Møller og Martin Harrow — Banedanmark
- Kirsten Kornerup — Lokalbanen

Kgs. Lyngby, december 2015

Nijs Jan Duijm

Seniorforsker

Indhold

Summary

This report presents guidance on structured hazard identification (HAZID) methods that can be used during risk assessment in the railway sector as required by the European Commission's Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment (CSM-RA), with later amendments.

The aim is to provide guidance on methods and on how to use these methods so that "proposers" (railway undertakers, infrastructure managers or other actors) are able to identify all reasonably foreseeable hazards that may exist in connection to the system changes being proposed. The proposer's demonstration of the proper use of such structured methods should give assessors sufficient confidence that the proposer indeed has identified all those hazards.

This guidance discusses the scope of hazard identification in the framework of CSM-RA, best practice in using workshops for hazard identification, and it presents four different structured methods. The two first methods are fundamental methods for performing HAZID "from scratch" (HAZOP and FMEA), the third method is the popular use of check lists, and reusing hazard identifications from earlier, similar projects is presented as a fourth, separate approach. The guidance concludes with discussing the application of HAZID methods on organizational and operational changes.

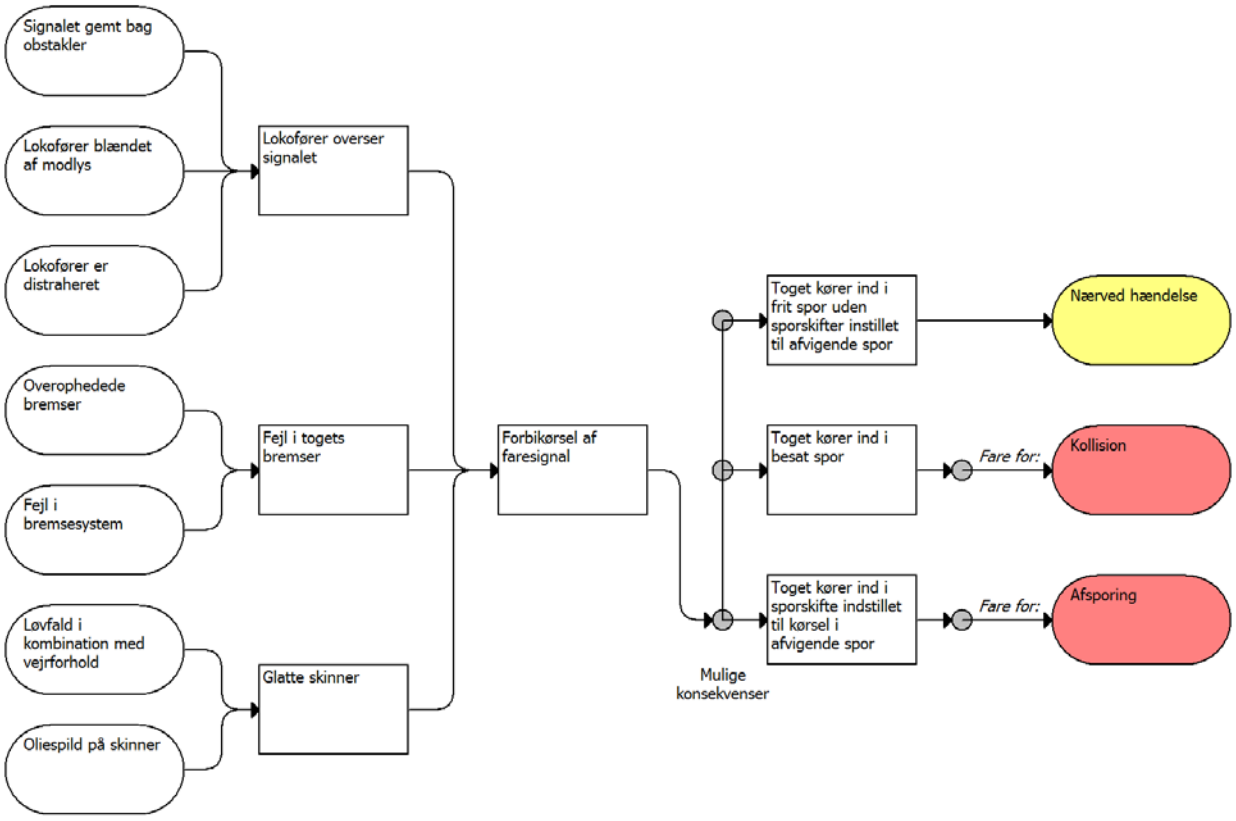
Key words: Railway, risk assessment, hazard identification

1. Introduktion

Fareidentifikation er en del af risikostyringsprocessen, som er foreskrevet af CSM-RA-forordningen (European Commission, 2013), bilag I, punkt 2.2.1 til 2.2.6. Denne vejledning præsenterer forskellige teknikker for at gennemføre en systematisk og struktureret fareidentifikation. Forskellige fareidentifikationsmetoder betegnes ofte som ”HAZID”-metoder, som forkortelse for den engelske betegnelse ”hazard identification”.

1.1 Farebegrebet

”Fare” er et ofte anvendt, men ikke tydeligt begreb. CSM-RA-forordningen definerer fare som (artikel 3, nr. 13): ”en situation, der kunne føre til en ulykke”. En ”fare” ses som potentialet for at der opstår en situation eller hændelse, som kan være en direkte årsag til en ulykke. Farer er i de fleste tilfælde relateret til en eller anden form af ”energi” (hastighed, varme, elektricitet, vægt, aggressivitet) som kan forvolde skade, hvis den ikke er under kontrol.



Figur 1 Eksempler af mulige farlige hændelsesforløb, dvs. forløb som kan føre til ulykker.

Farebegrebet illustreres ved hjælp af de mulige hændelsesforløb som er vist i Figur 1. De røde blokke til højre er ulykker. Alle blokke i midten (dem med de rette hjørner) er farer eller farlige situationer, som kan, men ikke nødvendigvis vil, føre til en ulykke (med udtagelse af ” Toget kører ind i frit spor uden sporskifter indstillet til (kørsel i) afvigende spor”, som kun fører til en ”nærved hændelse”). Blokkene til venstre kan opfattes som årsager til de farer til højre.

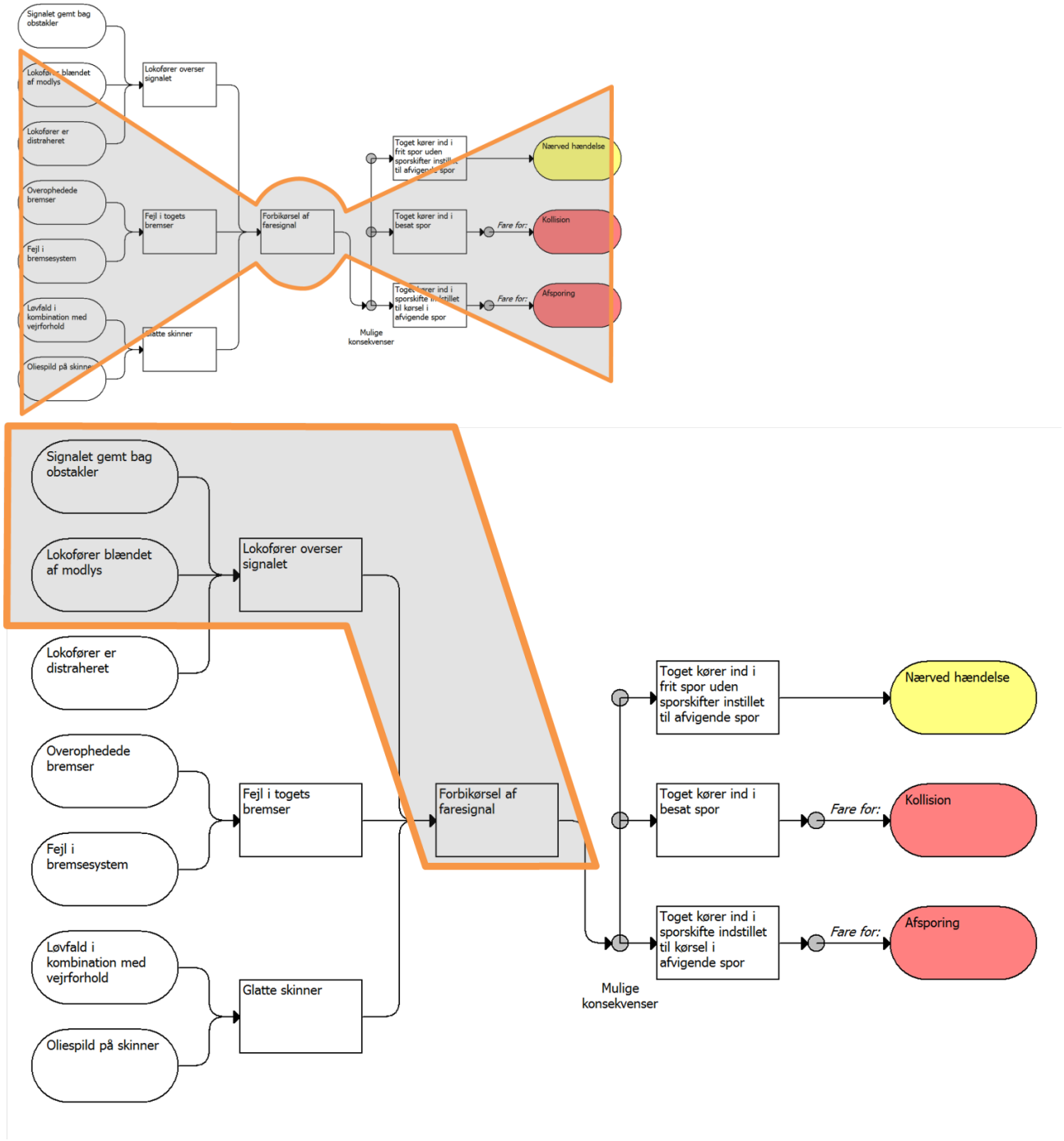
Det kan ses at der ikke er en enkelt hændelse eller situation, som kan betegnes som den ”eneste” eller ”rigtige” fare: farlige situationer er mulige årsager til andre farlige situationer (som er mere alvorlige, eller ”tættere” på ulykken).

Og det hvad der er præsenteret som ”årsager” kan ofte også opfattes som fare, da der ofte vil være ”årsager bag årsager”. Fx kan den *fare,* at et ”signal er gemt bag forhindringer” skyldes at:

- Signalet er placeret uhensigtsmæssig (bag en bro), eller
- Man har glemt at beskære buske og træer rettidigt, eller
- Der er oprettet et midlertidigt stillads, eller
- Osv.

Men man skal generelt opfatte farebegrebet fleksibelt, og det afhænger også den valgte fareidentifikationsteknik, hvad der anses for at være faren. Så vil ”faren” ved anvendelse af en FMEA (beskrevet i kapitel 5) nok identificeres som ”fejl”, fx i elementerne i togets bremsesystem, mens en HAZOP (beskrevet i kapitel 4) vil vurdere ”Tog bremser ikke eller for lidt” som en afvigelse af togets bremsefunktion, og en tjekliste (kapitel 6) vil måske direkte pege på overophedede bremser. Men ved alle tre metoder vil man ikke begrænses til at identificere ”faren” alene, men også søge efter årsager og konsekvenser, således at alle metoder i sidste ende vil kunne føre til samme ulykkesbeskrivelse. Formål med fareidentifikation er at identificere alle plausible farer i forbindelse med en ændring på et jernbanesystem.

Opstillingen i Figur 1 er vist i form af en såkaldt ”bow-tie”, dvs. at alle hændelser passerer én central fare i midten. Denne fare kaldes ofte for kernefaren eller den kritiske fare, se Figur 2. Kernefaren opfattes ofte som den fare som til sidst udløser ulykken. Dette skal heller ikke opfattes for strikt, der er ofte andre betingelser der bestemmer om der vil ske en ulykke, som vist i figuren, fx om sporet er besat, eller hvordan sporskifter er stillet, og også i disse situationer kan ulykker undgås ved tilfældigheder. Dette for at forklare, at *faren* ikke er identisk med *ulykken*.



Figur 2 Mulige hændelsesforløb tegnet som en "bow-tie" med "forbikørsel af faresignal som kernefare.

"Fare" forveksles også nemt med "risiko". Begrebet "risiko" går et skridt videre end fare. Farens risiko omfatter både farens mulige konsekvens, dvs. resultatet af den mulige ulykke, men også sandsynligheden for, at ulykken indtræffer. En fare kan være alvorlig, men dens risiko kan være lille.

1.2 Afgrænsning af fareidentifikation i forhold til CSM-RA

Farer skal i denne sammenhæng betragtes som forhold, der kan føre til en ulykke. "Ulykke" kan her forstås som enhver ulykke, som resulterer i mindst én dræbt eller alvorligt tilskadekommen person, eller i omfatten-

de ødelæggelse af materiel, spor eller andre anlæg og miljøet eller i omfattende forstyrrelse af trafikken. Nedenfor findes en ikke-udtømmelig liste over potentielle ulykkeskategorier:

- Sammenstød mellem tog og jernbanekøretøjer;
- Togsammenstød med forhindringer inden for fritrumsprofilen;
- Afsporinger;
- Ulykker i jernbaneoverkørsler, herunder ulykker, der involverer fodgængere på jernbaneoverkørsler
- Personulykker, der involverer rullende materiel i bevægelse;
- Brande i rullende materiel;
- Andre (dvs. alle andre ulykker som er dækket af direktivets definition af en ulykke);

Fareanalysen kan begrænses til at betragte følgende persongrupper:

- Jernbanepassagerer;
- Ansatte i jernbanevirksomheder (infrastrukturansvarlige og operatører);
- Tredjepart som kan komme i kontakt med jernbanens systemer (ved overkørsler, på stationer, rangerområder osv.),

Arbejdsulykker ved fabrikation, konstruktion og installation af jernbanens systemer, som foregår udenfor, og afskærmet fra den daglige jernbanedrift, er ikke omfattet af CSM-RA.

1.3 Vejledningens formål

Resultatet ved fareidentifikationen skal være en liste med alle plausible farer, der med rimelighed kan forudses[1]. Det er umuligt at bevise, at en liste med farer er udtømmende. Derfor lægges der vægt på, at fareidentifikationen gennemføres via en proces, som med rimelighed kan sikre, at ingen relevante farer overses. Dette forudsætter, at processen er struktureret og/eller at der gøres brug af metoder eller data (fx tjeklister), som er udtømmende. Med *udtømmende* menes i denne sammenhæng, at disse data (fx tjeklister) bør omfatte alle tilgængelige oplysninger, som er relevante for det system eller den ændring som skal risikovurderes[2].

Formål med denne vejledning er derfor at præsentere metoder, som kan leve op til disse krav om at være *strukturerede* og *udtømmende*. Derudover bør processen altid dokumenteres på en sådan måde, så assessor kan blive overbevist om, at processen er udført på en måde, således at resultatet (dvs. listen med farer) med rimelighed må formodes at være udtømmende for det pågældende system. Vejledningen indeholder derfor anbefalinger til, hvordan man anvender fareidentifikationsmetoder, og hvordan både processen og resultatet dokumenteres.

Fareidentifikationen kan (bør) omfatte selve identifikationen og en klassificering af farerne (DTA, 2010). CSM-RA-forordningen forventer i forbindelse med fareidentifikationen, at forslagsstiller afgør, om faren er alment accepteret. Det kan diskuteres, om klassificeringen kan foretages uden en risikovurdering – det kræver både en vurdering af de mulige konsekvenser og sandsynlighed. CSM-RA-forordningen lægger ansvaret over på en ”ekspertvurdering”.

---

[1] Jf. CSM-RA-forordningen nr. 402/2013 Bilag I, punkt 2.2.1.

[2] Jf. CSM-RA-forordningen nr. 402/2013, artikel 3, punkt 2: definition af risikoanalyse: systematisk anvendelse af alle tilgængelige oplysninger til at identificere farer og estimere risikoen

Fareidentifikation er en delvis iterativ proces, som ikke kan ses adskilt fra risikovurderingen og vurderingen af sikkerhedsforanstaltninger (Jovicic, 2009). Det britiske Office of Rail and Road (ORR, 2015) foreslår, at man starter ved at betragte farer på et højere abstraktionsniveau; kan faren kontrolleres på det niveau, er det ikke nødvendigt at nedbryde årsager på lavere niveau[3].

[3] Jf. CSM-RA-forordningen nr. 402/2013 Bilag I, punkt 2.2.5

2. Generel fremgangsmåde ved fareidentifikation

2.1 Inddragelse af erfaring og nærved/ulykkesregistreringer

Denne vejledning fokuserer på beskrivelser af metoder til på systematisk vis at "opfinde" farer baseret på en systemdefinition. Men det må ikke forbigås, at hændelser i det virkelige liv er en vigtig kilde af viden og inspiration. Det anbefales derfor, at fareidentifikationen også omfatter en gennemgang af databaser og registreringer med ulykker og/eller nærved hændelser med henblik på at identificere farer, som er relevante for det system, der skal risikovurderes. Mange hændelsesbeskrivelser indeholder også "lessons learned" med forslag til sikkerhedsforanstaltninger.

Oplysninger om jernbaneulykker og -hændelser kan hentes fra forskellige kilder, herunder virksomhedens egne registreringer og ved henvendelse til Trafiks- og Byggestyrelsen eller Havarikommissionen. De fleste lande i EU har lignende organisationer, som udgiver hændelsesrapporter af ulykker og hændelser, nogle af dem udgiver (sammenfatninger) på engelsk. En liste med disse kilder er tilføjet i Bilag B til denne vejledning.

Det bør bemærkes, at det er svært at navigere rundt i de fleste af disse databaser. Søgemulighederne på de forskellige websider er forskellige, hvilket gør, at det kan være svært at søge efter hændelser relateret til en bestemt systemtype eller driftstype. De fleste databaser kan ordnes efter type af ulykke, som fx afsporing eller kollision, men det er svært at lede efter bestemte hændelsesårsager, da disse er "gemt" i rapporteringstekster, som ofte foreligger i pdf. En systematisk gennemgang af disse databaser kan derfor næppe kræves som del af en systematisk fareidentifikation.

ERAIL tillader at søge efter "causal factors" og "occurrence type", og det anbefales derfor, at der foretages en systematisk søgning i ERAIL forud for en fareidentifikation, hvis der er overlap mellem systemet og disse søgekriterier.

2.2 Workshop

CSM-Forordningen (European Commission, 2013) kræver, at der til fareidentifikationen hentes viden fra et team (Bilag I, punkt 2.2.1). Fareidentifikation foreslås derfor udført ved, at teamet samles i en workshop af én eller flere sessioner. Et fareidentifikationsteam bør efter bedste praksis i fx procesindustri bestå af:

- En ordstyrer. Ordstyreren skal have kendskab til fareidentifikationsmetoden, og det er ordstyrerens ansvar, at processen udføres systematisk og i overensstemmelse med minimumskrav til metoden, herunder dokumentation af processen, således at resultatet af fareidentifikationen er en dækkende og relevant liste med systemets farer;
- En skribent, som har til opgave at registrere alle relevante farer, som bliver identificeret i løbet af fareidentifikationsprocessen. Skribenten skal, i samarbejde med ordstyreren, sikre at deltagerne er enige i registreringen;
- Mindst 3 og helst ikke mere end ca. 8 deltagere, som tilsammen har kompetencerne til at afdække alle faglige områder, som er relevante for den ændring, der skal risikovurderes. Deltagerne skal helst repræsentere forskellige tilgangsvinkler til projektet, såsom udvikling, konstruktion, operation, brugere og vedligehold.

Bemærk, at det er deltagerne, som tilfører processen den nødvendige faglige viden. Det er ikke nødvendigt (men kan være en fordel), at ordstyrer og skribent har en dybtgående faglig viden om emnet, ligesom det ikke er nødvendigt (men kan være en fordel), at deltagerne har erfaring med fareidentifikationsprocessen.

Ordstyreren skal fremprovokere, at alle deltagerne foreslår farer og potentielle hændelser. Intet forslag må afvises direkte. Kun hvis deltagerne er enige om, på baggrund af objektive argumenter, at nogle forslag ikke er relevante eller urealistiske, registreres forslaget ikke i fareregistret. Hvis der ikke opnås enighed, registre-

res forslaget, og der kan tilføjes, at faren skal undersøges nærmere. Faren kan efterfølgende muligvis lukkes (ikke fjernes) i registret med henvisning til en nærmere undersøgelse, som viser, at hændelsen ikke kan ske.

Fareidentifikation kan være en tidskrævende proces. For at sikre, at de farligste dele af et projekt prioriteres, kan ordstyreren i samråd med deltagerne beslutte i hvilken rækkefølge elementerne behandles.

Ved begyndelsen af workshoppen skal ordstyreren introducere processen og forklare den fareidentifikationsteknik, der skal bruges.

2.3 Teamets sammensætning

For at gruppen har den fornødne synergi og samspil til at generere farer, foreslås, at der mindst skal være 3 fagligt kompetente deltagere i gruppen, udover ordstyreren. Skribenten kan i en mindre gruppe også optræde som faglig deltager.

På grund af praktiske overvejelser skal gruppen heller ikke være for stor, og derfor foreslås det, at der ikke inviteres mere end ca. 8 faglige deltagere til sessionerne. Bemærk, at fareidentifikationen kan strækkes over flere sessioner, og deltagerne behøver ikke (alle) at være de samme for hver session. Der kan inviteres bestemte eksperter, når forskellige dele af projektet behandles. Det frarådes at udskifte alle deltagere per session med henblik på at fastholde kontinuitet i processen. Nye deltagere skal have kendskab til de tidligere identificerede farer for at undgå gentagelser.

Teamet skal dække de faglige områder og grænseflader som er relevant for vurdering af den foreslåede ændring. Teamet skal helst omfatte både designere, brugere og fageksperter. Det er vigtigt, at deltagerne er bevidste om deres kompetencer og især også begrænsninger af deres kompetencer. Risikoanalyser er defineret som ” systematisk anvendelse af alle tilgængelige oplysninger til at identificere farer og estimere risikoen”[4]. Deltagerne skal sikre adgang til disse oplysninger, men ingen kan vide alt. Det er derfor vigtigt, at deltagerne markerer, hvornår der er behov for at indhente ekstra oplysninger. Det kan i dokumentationstabellen markeres som en aktion, at der indhentes ekstra oplysninger, når workshoppen er afsluttet, og disse oplysninger bruges i den senere risikoanalyse.

Ordstyreren, som har det overordnede ansvar, må forsøge, hvis det er muligt, at sikre, at teamet ikke er domineret af enkeltindivider, enten på grund af personlighed eller på grund af organisatorisk-hierarkiske forhindringer. Ordstyreren bør under workshoppen sikre, at der er balance mellem bidrag fra de mere fremtrædende og mere tilbageholdende deltagere. Det anbefales hver gang at inddrage nogle nye deltagere med ingen eller mindre erfaring med fareidentifikation for at forhindre, at processen bliver til rutine.

For at demonstrere at teamet, som bidrager til fareidentifikationen, er kompetent efter CSM-RA-forordningens krav[5], foreslås at deltagernes kompetencer dokumenteres på følgende måde:

- Navn og ansættelse (arbejdsgiver og stilling)
- Begrundelsen for deltagelse; enten en relevant faglig kompetence, og/eller fordi pågældende repræsenterer en aktør (bruger, operatør, vedligeholdsmedarbejder o.l.);
- Deltagerens erfaring med den kompetence eller i den rolle (fx antal år i relevant stilling og/eller uddannelse og træning, erfaring fra lignede projekter)

[4] Jf. CSM-RA-forordningen nr. 402/2013, artikel 3, nr. 2

[5] CSM-RA-forordningen nr. 402/2013 Bilag I, punkt 2.2.1

2.4 Baggrundsmateriale: systemdefinition

Fareidentifikationen baseres på systemdefinitionen. Systemdefinitionen, og dertil hørende yderligere dokumentation af (del)systemer fx tegninger, bør være tilgængelige for alle deltagere i workshoppen. Fareidentifikationen afhænger af systemdefinitionens kvalitet. Det skal være afstemt, at systemdefinitionen passer med den fareidentifikationsmetode, som er valgt, især med henblik på detaljeniveauet. Det må kræves af deltagerne, at de har gennemgået systemdefinitionen nøje, inden workshoppen afholdes.

Systemdefinitionen skal i henhold til CSM-RA-forordningen punkt 2.1.2 indeholde et afsnit om antagelser. Fareidentifikationen skal vurdere i hvilken udstrækning disse antagelser påvirker mulige farer, dvs. at man skal tage stilling til, om en ændring i antagelsen kan medføre en (forholdsvis stor) ændring i fare (eller risiko ved faren).

2.5 Registrering af farer under workshoppen

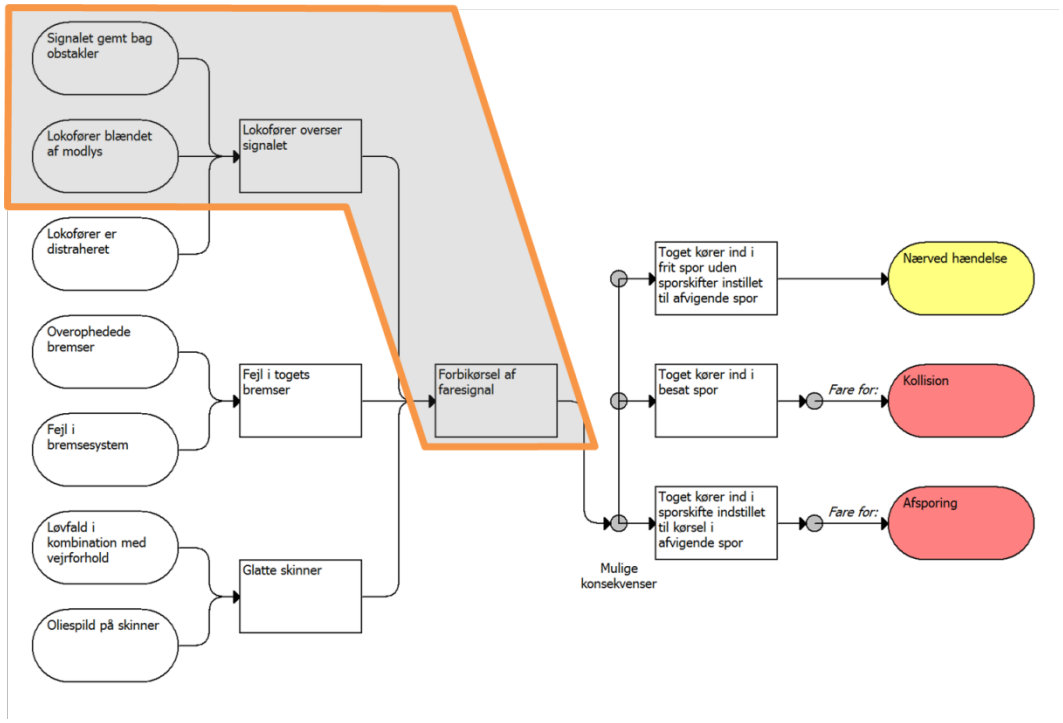
Under workshoppen noterer skribenten de identificerede farer med årsager, konsekvenser og (eksisterende) sikkerhedsforanstaltninger. De fleste standardiserede fareidentifikationsteknikker foreslår et bestemt tabelformat for at notere farer. CSM-RA-forordningen kræver, at forslagsstilleren løbende skal føre et fareregister[6]. Det er en selvfølge, at dette fareregister (herefter betegnet som ”projektets fareregister”) bør baseres på ovennævnte tabeller. Disse tabeller kan være basis for projektets fareregister – i så fald skal tabellerne udvides med felter for at følge op på risikovurderinger og aktioner gennem CSM-RA-processen. Alternativt overføres farerne fra workshoptabellen til projektets fareregister. Workshoptabellen er dermed workshoppens ”referat” og opdateres efter endelig redigering ikke (opdateringer sker i projektets fareregister).

Workshoptabeller kan udfyldes i regneark (Microsoft Excel ® eller lignende), men der findes også frit tilgængelige og kommercielle software-værktøjer til dokumentation af fareidentifikationer, som indeholder skabeloner for forskellige teknikker (fx PHA Pro, Isograph, ReliaSoft).

2.6 Afgrænsning af fareidentifikationen

Fareidentifikationen bør begrænses til kun at omfatte de farer, som er relateret til det system, eller den systemændring, som skal vurderes. Disse farer kan sagtens have påvirkning udenfor det vurderede system, eller systemændringen kan medføre farer i andre systemer, og disse farer bør selvfølgelig inkluderes. Men ellers er det ordstyrerens opgave at sikre, at workshoppen forbliver fokuseret. Det illustreres ved følgende figurer, som er baseret på Figur 1. Hvis en systemændring omfatter placering eller ændrede forhold omkring et signal, så er de farer, der er indrammet i Figur 3 relevante. Selvom vurderingen bør tænke ergonomien i forhold til synligheden af signalet, er faktorer som vedrører lokomotivførerens andre opgaver, indretning af førerkabinen osv. ikke relevante, da den infrastrukturelle ændring ikke ændrer på dette.

[6] CSM-RA-forordningen nr. 402/2013 Bilag I, punkt 1.1.3

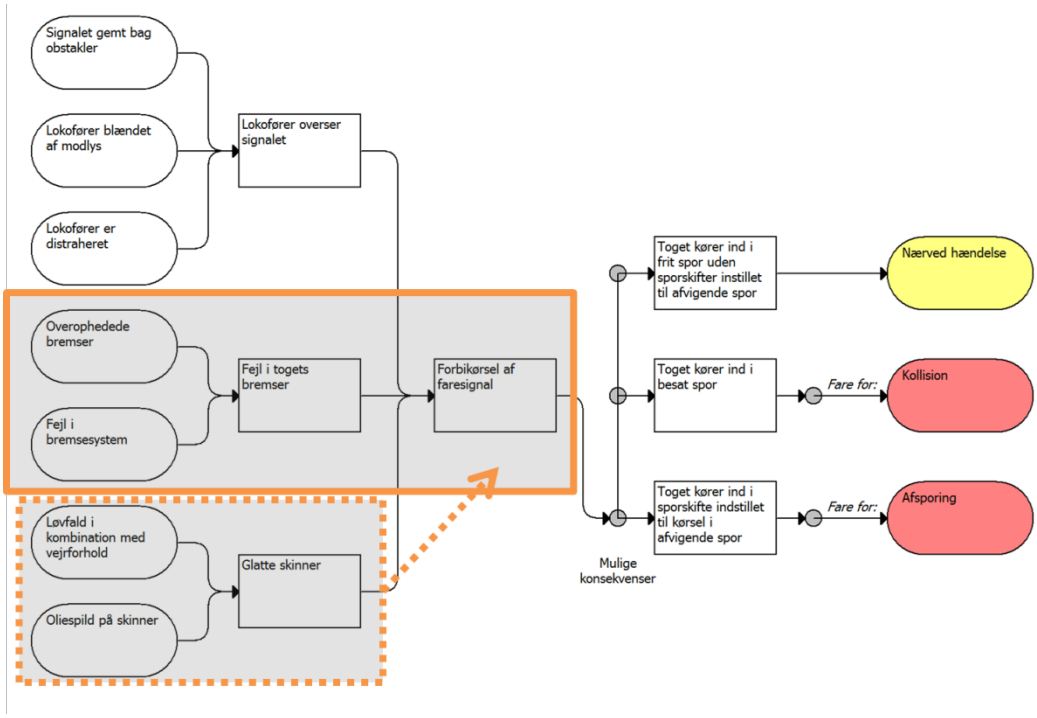


Figur 3 Relevante hændelser når placering af et signal vurderes

Et andet eksempel vises i Figur 4. Ændringer i rullende materiel bør ikke betragte andre farer eller årsager som kan føre til forbikørsel, end dem, der vedrører det rullende materiel selv. Ændringer i rullende materiel kan ikke påvirke årsager til andre farer, som fx glatte skinner. I de fleste tilfælde vil der være formuleret et krav om tilstrækkelig bremsekraft, også ved mindre gode forhold, som glatte skinner. Dvs. at risiko i forbindelse med glatte skinner i forhold til bremsesystemet er dækket af en kravspecifikation. Ved udvikling af fx et helt nyt togsæt kunne det eventuelt tænkes at fastsættelse af denne kravspecifikation også er underlagt en (separat) risikovurdering.

En anden afgrænsning vedrører, hvor langt man skal gå med at lede efter årsager: i princippet har hver årsag en bagvedliggende årsag, og denne søgning kan blive ved. Med henvisning til CSM-RA-forordningen[7] er det kun nødvendigt at udføre fareidentifikationen til det -niveau af årsager, hvor man kan indføre sikkerhedsforanstaltninger, som fjerner eller minimerer disse årsager, således at de medfølgende farer er under kontrol. Man skal således allerede under workshopsessionen tage stilling til dette og finde en balance mellem detailniveau og tidsforbrug for workshoppen. Det nævnes i CSM-RA-forordningen at en iterativ proces mellem risikoanalyse og fareidentifikation kan være nødvendigt[7]. Det kan i praksis vise sig under risikoanalysen, at man ikke på tilstrækkelig vis kan kontrollere den årsag, som er beskrevet i fareregistret. På det tidspunkt er man nødt til at finde ud af, om der findes bagvedliggende årsager, som kan kontrolleres i stedet for. Denne øvelse vil i praksis kun involvere en mindre gruppe eksperter og kan næppe betragtes som en ”genoptagning” af fareidentifikationen.

[7] CSM-RA-forordning en nr. 402/2013, Bilag I, punkt 2.2.5.



Figur 4 Relevante hændelser som vedrører ændringer i rullende materiel. Bremsesystemet skal opfylde krav i forhold til skinnernes tilstand (glathed, friktion), men årsager til glatte skinner kan ikke løses ved ændringer i rullende materiel.

2.7 Omfang af workshop

Alle fareidentifikationsmetoder har først og fremmest som formål:

1. Identifikation af alle farer (eller fejl, eller afvigelser, betegnelsen afhænger af den valgte metode), som ændringen kan medføre;
2. Identifikation af årsager til disse farer;
3. Identifikation af mulige konsekvenser af disse farer.

Den generelle opfattelse er, at mens gruppen af eksperten er samlet på workshoppen, og der er opmærksomhed på faren, så bruges dette til samtidig at identificere eksisterende og mulige forebyggende og risikobegrænsende foranstaltninger: alle skemaer til fx HAZOP og FMEA indeholder en kolonne, hvor disse foranstaltninger registreres. Dette er den anbefalede fremgangsmåde i de fleste industrier. Det kan dog overvejes, at identifikation af risikobegrænsende foranstaltninger planlægges separat for at holde workshoppens team fokuseret på farer og for at undgå at teamet kommer i "løsningsmode".

2.8 Farer som indebærer "Alment accepterede risici"

Ifølge CSM-RA-forordningen[8] skal der under fareidentifikationen foretages en klassificering af de identificerede farer, ud fra hvilke man kan beslutte, om de risici som disse farer indebærer, skal analyseres yderligere i den efterfølgende risikoanalyseproces. Farer som kun indebærer "alment accepterede" risici behøver ikke at blive analyseret yderligere.

[8] CSM-RA-forordningen nr. 402/2013, Bilag I, punkt 2.2.3.

Ifølge forordningen skal alle farer, også dem som indebærer alment accepterede risici, registreres i fareregistret.

Det kan diskuteres om det er muligt uden en nærmere analyse at konkludere om risici er alment accepterede. Ifølge forordningen menes med ”alment accepterede risici”, at de er så små, at det ikke er rimeligt at gennemføre yderlige sikkerhedsforanstaltninger[9]. Sådanne overvejelser kan være for komplekse til, at man kan håndtere dem på en fareidentifikationsworkshop. Der er intet til hinder for, at man udsætter sådanne klassificeringer til efter fareidentifikationen. (Formelt set vil det betyde at fareidentifikationen klassificerer alle farer som til at kræve yderlige analyse: den yderlige analyse kan fastslå at der er farer som ikke kræver sikkerhedsforanstaltninger).

Det påpeges at denne klassificering af farer *kun* udføres for farer som *ikke* kontrolleres af allerede tilstedeværende eller planlagte sikkerhedsforanstaltninger. Da eksisterende eller planlagte sikkerhedsforanstaltninger må forventes at være ”rimelige”, vil det betyde at farer kontrolleret af disse foranstaltninger, *uden* disse sikkerhedsforanstaltninger medfører risici som *ikke* er alment accepterede. Farer bør indgå i fareregistret sammen med en beskrivelse af de eksisterende eller planlagte sikkerhedsforanstaltninger, og indgå i CSM-RA-risikostyringsprocessen.

2.9 Undgå faldgruber ved fareidentifikation

Ved fareidentifikation skal man være opmærksom på følgende:

- Fareidentifikationsprocessen og workshoppen bør være ordentligt forberedt, planlagt, og de nødvendige ressourcer bør være til rådighed, dvs. at processen har den nødvendige prioritering i organisationen. Ordstyreren har ansvar for, at alle deltagerne har adgang til dokumentation i god tid, at deltagerne på forhånd er instrueret i processen, og at de nødvendige faciliteter er til rådighed. Skribenten er forberedt til at dokumentere og har praktisk øvelse i det registreringsværktøj, som skal anvendes. Deltagerne har læst og forstået dokumentationen.
- Processen bør være struktureret. Det er ordstyrerens opgave at lede teamet på struktureret måde systematisk gennem:
  - Alle aspekter eller delelementer af systemet eller systemændringen
  - Alle guideord eller emner fra tjeklisten
  - Alle relevante årsag af de fundne farer
  - Alle relevante konsekvenser af de fundne farer
- Processen bør fokuseres på den foreslåede ændring. Det er ordstyrerens opgave at holde teamet fokuseret, og at teamet ikke kører ”ud af en tangent”
- Alle kompetencer bør udnyttes; det er ordstyrerens opgave at se til, at alle deltagere får mulighed for, og bliver opfordret til at bidrage.
- Alle nævnte farer skal dokumenteres.
- Skribenten bør sikre sig, at hvad der skrives ned, gengiver deltagernes input på korrekt vis. Det er en fordel at teamet kan læse hvad der bliver noteret ved at vise rapporteringstabellen på en storskærm. Nogle ordstyrere bruger op til tre skærme eller projektorer: én til at vise tabellen, én til tegninger og dokumentation, og én til at vise eksempler på farer eller ulykker

[9] CSM-RA-forordningen nr. 402/2013, Bilag I, punkt 2.2.3.

- Undgå for mange forkortelser i dokumentationen og fareregistret: det skal også være forståeligt for personer udenfor teamet, og forkortelserne skal kunne huskes efter længere tid.
- Man bør undgå, at sessionerne varer for længe. Sessioner, som varer længere end ca. 3 timer vil ikke længere være produktive. Det frarådes at afholde flere sessioner på samme dag.

3. Introduktion af fareidentifikationsmetoder

I de følgende fire kapitler præsenteres forskellige metoder til fareidentifikation. De første to (HAZOP, Hazard and Operability Analysis og FMEA/FMECA, Failure Mode and Effect (and Criticality) Analysis) er metoder som bruges når fareidentifikationen er krævet "fra bunden". De er i høj grad strukturerede og beskrevet i standarder (eller standardiserede vejledninger). De kræver en ordstyrer i workshoppen (kapitel 2), som har indgående kendskab og erfaring i hhv. HAZOP eller FMEA/FMECA, og de plejer at være tidskrævende. De er egnede til komplekse systemændringer, ved anvendelse af nye, innovative løsninger som ikke har været risikovurderet før, eller når der er usikkerhed om mulighed for at overse farer, hvis man vil anvende mindre stringente fareidentifikationsmetoder.

De sidste to metoder, tjeklister og genbrug af resultater fra tidligere fareidentifikationer, anvendes i situationer hvor systemerne og systemændringerne er kendte, og hvor man har opnået tilstrækkelig indsigt i farer fra tilsvarende projekter. Disse metoder er mindre ressourcekrævende, og bygger på genbrug af viden fra tidligere fareidentifikationer.

De præsenterede metoder er komplementære; brug af en bestemt metode må aldrig være undskyldning for at overse åbenlyse farer. Selvom man på forhånd har valgt en bestemt metode, anbefales det at gennemgå nedenstående beskrivelser af alle metoder for at få et alment indblik i fareidentifikationsprocessen. En stor del af overvejelser, fx omkring forhold mellem fare, årsag og konsekvens, ved anvendelse af HAZOP og FMEA, bruges også ved anvendelse af tjeklister.

Det er et bevidst valg først at beskrive og præsentere de "store" metoder, HAZOP of FMEA. Tjeklistemetoden bygger især på HAZOP metoden, for eksempel når det gælder opdeling af systemet med henblik på en struktureret gennemgang, og det anbefales at læse det pågældende afsnit under HAZOP. Genbrugsmetoden bygger videre på en eksisterende fareidentifikation, som er gennemført med én af de fornævnte metoder: Det forventes at man vil bruge den samme metode til det nye studie.

Alle metoder, som er præsenteret, kan anvendes på de forskellige mulige systemændringer: tekniske, driftsmæssige og organisatoriske. Der er stor erfaring i anvendelse af HAZOP, FMEA/FMECA og tjeklister for tekniske systemer. I kapitel 8 beskrives anvendelse på organisatoriske ændringer og ændringer i forhold til driftsprocedurer og beskrivelser af arbejdsopgaver.

Valg af fareidentifikationsmetode afhænger af kompleksiteten i ændringen, om der gøres brug af nye, ikke-afprøvede løsninger og ændringens farepotentiale. Med hensyn til farepotentialet kan der sondres mellem, om ændringen ville kunne udsætte flere personer for fare samtidig (dvs. der er mulighed for en katastrofal ulykke) eller om der kun udsættes en enkelt eller en mindre gruppe af personer for fare (dvs. der er højst mulighed for en kritisk ulykke). Tabel 1 viser hvilke metoder der er mest egnet i en bestemt situation.

Tabel 1 Oversigt over egnede fareidentifikationsmetoder afhængig af kompleksitet og innovationsniveau.

++ Anbefalet metode

+ Egnet metode

o Brugbar, men ikke anbefalet metode

- Ikke brugbar metode

Type af ændring	**Fareidentifikationsmetode**			
	HAZOP	FMEA/-FMECA	Tjekliste	Genbrug
Ændring i et velkendt system som kun i mindre grad involverer nye, ikke-afprøvede løsninger (fx ændring som forventes at kunne risikovurderes ved hjælp af anerkendt praksis)	o	o	++	-
Ændring som involverer nye, ikke-afprøvede løsninger og med potentialet for en katastrofal ulykke	++	++	o	-
Ændring som involverer nye, ikke-afprøvede løsninger og med potentialet for en kritisk ulykke	+	+	++	-
Brug af en ny (del)komponent (software, hardware) i et ellers velkendt system med potentialet for en katastrofal ulykke	o	++	+	-
Brug af en ny (del)komponent (software, hardware) i et ellers velkendt system med potentialet for en kritisk ulykke	o	+	++	-
Ændring som er kompleks og måske mangler en klar afgrænsning med omgivende systemer (mange grænseflader og interaktioner)	++	o	o	-
Ændring som er næsten identisk med en tidligere gennemført ændring, og hvor der foreligger en fareidentifikation for den tidligere ændring	o	o	+	++

4. Metode 1: Funktionsorienteret metode ved hjælp af HAZOP guideord

HAZOP er en anerkendt metode i mange tekniske domæner, især procesorienterede domæner. For at metoden kan anvendes på jernbaneområdet, bør man have overvejet, hvordan ”processen” i jernbaneområdet formuleres, for at HAZOP kan anvendes med succes. Derfor beskrives i de følgende afsnit den ”oprindelige” HAZOP, som den anvendes i især procesindustrien. Bagefter beskrives i afsnit 4.2 hovedprincipperne i Functional Hazard Analysis (FHA), som er oplagt at kombinere med HAZOP metoden, mens afsnit 4.3 beskriver den anbefalede metode, som anvender HAZOP-metoden på systemelementernes funktioner.

4.1 Oprindelige HAZOP metode

HAZOP (HAZard and OPerability study) er en fareidentifikationsmetode, som i 1963 blev udviklet af ICI (UK). HAZOP er udviklet til procesindustri, dvs. systemer som består af rør, pumper og beholdere, hvori bestemte stoffer cirkulerer.

HAZOP-metoden er proces- eller funktionsorienteret og deduktiv (”top-down”): det store system deles op i nogle få systemelementer, som kan beskrives med en enkel, utvetydig funktion (fx: transport, opbevaring, opvarmning, …). Metoden går ud på at identificere mulige afvigelser i processen (for meget, for lidt, for sent), og bagefter finde ud af de mulige *årsager* til disse afvigelser, og hvilke *konsekvenser* afvigelsen muligvis kan medføre. Metoden bruger en liste med 11 såkaldte guideord (”guide words”) for at generere mulige afvigelser, se Tabel 1. Det, at man på systematiskvis kan generere disse afvigelser og derefter kan tage stilling til om de er relevante, gør, at metoden er struktureret.

Afvigelserne genereres ved at anvende alle guideord efterfølgende på relevante egenskaber eller karakteristikker af det systemelement, man kigger på:

Guideord + karakteristik = afvigelse.

For eksempel hvis vi ser på en batteri, så er funktionen at levere elektrisk kraft. Den elektriske kraft kan karakteriseres ved spænding og strøm. Derfor kan man generere kombinationerne med guideord "MERE":

- MERE + Strøm = (for) høj strømstyrke (fx forårsaget af kortslutning)
- MERE + Spænding = (for) høj spænding

Og med ”OMVENDT”:

- OMVENDT + Strøm = opladning (i stedet for at levere kraft)
- OMVENDT + Spænding = forkert polaritet

Tabel 2 HAZOP "guideord" og deres betydning. I højre kolonne er de oprindelige engelske guideord.

	Guideord Dansk	Betydning	Guideord Engelsk
Grundlæggende guideord	INGEN/INTET	Fuldstændigt fravær af det planlagte formål	NO OR NOT
	MERE/FLERE	Kvantitativ stigning	MORE
	MINDRE/FÆRRE	Kvantitativ nedsættelse	LESS
	UDOVER	Kvalitativ ændring, i tillæg til	AS WELL AS
	DELVIS	Kvalitativ ændring, mangler	PART OF
	OMVENDT	Logisk omvendt resultat i forhold til det planlagte formål	REVERSE
	I STEDET FOR	Fuldstændig erstatning	OTHER THAN
Guideord relateret til tid eller rækkefølge	TIDLIG	I forhold til klokkeslæt	EARLY
	SEN	I forhold til klokkeslæt	LATE
	FØR	I forhold til rækkefølge	BEFORE
	EFTER	I forhold til rækkefølge	AFTER

Den oprindelige HAZOP-metode er beskrevet i vejledning 61882 fra den International Electrotechnical Committee (IEC, 2001). Der findes instruktive bøger, som forklarer HAZOP, inklusive god praksis og faldgruber, og som sammenligner med andre metoder, der kan anbefales når man ønsker at anvende denne HAZOP- eller en HAZOP-lignende metode (Crawley, Preston, & Tyler, 2000; Kletz, 1999). HAZOP-metoden kan overføres til andre domæner end procesteknologi, og det kan lade sig gøre, hvis man er i stand til at definere funktioner og/eller egenskaber af systemelementer, og man ved hjælp af guideordene systematisk kan gennemgå, hvad der sker, når disse systemelementer enten ikke opfylder funktionen, eller deres egenskaber afviger fra den ønskede tilstand. Ovennævnte vejledning fra IEC indeholder i dens anneks B2 et eksempel af anvendelse af HAZOP-metoden på en procedure, og i anneks B3 et eksempel for et Automatisk Tog Stop system, se også bemærkningen i afsnit 4.3 nedenfor.

4.2 Functional Hazard Analysis (FHA)

Den britiske Rail Safety and Standards Board (RSSB, 2014) henviser til en metode, som kaldes "Functional Hazard Analysis (FHA)". Der findes nogle få referencer i litteraturen, som nævner FHA, men ingen klar metodisk beskrivelse. Metoden baseres på en beskrivelse af funktioner i systemet, og det ligger lige for, at man kan bruge HAZOP-guideord, som beskrevet ovenfor, til at generere afvigelser, hvor funktioner udføres forkert, for sent, omvendt osv., situationer som på struktureret vis kan genereres ved hjælp af systematisk brug af disse guideord.

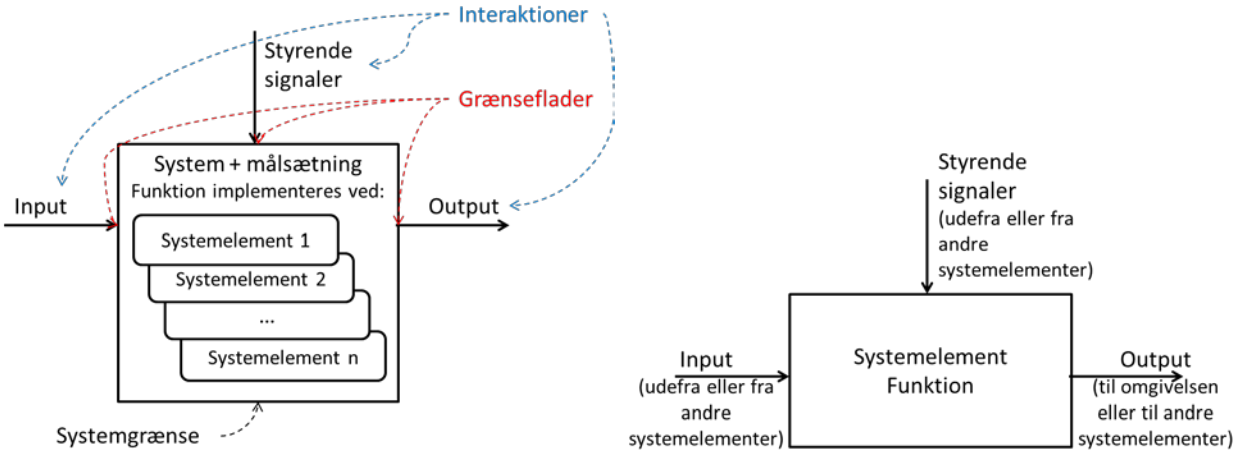
Det er nævnt, at der kun kan findes afvigelser i relation til funktionen, og at det ikke er sikkert, at en fokusering på funktionen belyser alle sikkerhedsrelevante forhold. Hvis det skal være succesfuldt, skal "funktionen" også omfatte eventuelt input og output (fysisk eller som information/data) og eventuelle tilstande (status) af de systemer, som leverer funktionerne, som beskrevet under HAZOP ovenfor.

4.3 Funktionsorienteret fareidentifikation ved hjælp af HAZOP-guideord

Inspireret af ovennævnte HAZOP-metode og FHA foreslås en kombination som indtil videre betegnes som "funktionsorienteret fareidentifikation ved hjælp af HAZOP-guideord". Metoden beskrives her.

Der tages udgangspunkt i systemdefinitionen. Systemdefinitionen indeholder beskrivelsen af (se Figur 5):

- Hovedsystem med definition af formål og funktion;
- Grænseflader af hovedsystem med interaktioner på tværs af grænseflader;
- Systemelementerne i hovedsystem med hver systemelements (del)funktion;
- Systemelementernes grænseflader og interaktioner, både dem som er sammenfaldende med hovedsystemets grænseflader/interaktioner, og systemelementerne indbyrdes.



Figur 5 Grafisk fremstilling af hovedsystem og systemelementer, som følger "ICOM" konventionen: *Input*, *Control* (styrende signaler), *Output* og *Methods* (implementering ved hjælp af de underliggende systemelementer).

En funktionsorienteret HAZOP tager udgangspunkt i systemelementerne, som implementerer hovedsystemet. HAZOP-metoden anvendes på interaktionernes input, output og de styrende signaler, dvs. der genereres for hvert systemelement en række afvigelser ved hjælp af følgende regler:

- Guideord + Input
- Guideord + Output
- Guideord + Styresignal[10]

Konkret betyder det, at man vælger en interaktion, definerer en af interaktionens karakteristikker, og kombinerer hver af de 11 guideord fra Tabel 1 på denne karakteristik for at se, om det giver en meningsfuld afvigelse og fare.

Der værnes selvfølgelig mod unødvendig duplikation: hvis input eller styresignal for ét systemelement er output fra et andet systemelement, behandles det kun én gang. Ligeledes vil ikke alle kombinationer af guideord og input/output være meningsfulde som afvigelse.

---

[10] Det er ikke nødvendigt at håndtere "styresignal" (kontrol) på en anden måde end øvrige input med hensyn til fareidentifikationen. Forskellen er bibeholdt for at opretholde overensstemmelse med ICOM-(Input, Control, Output, Methods)-konventionens måde at beskrive systemer eller delelementerne på.

Metoden kan anvendes, når hovedsystemernes succesfulde funktion fuldstændig kan beskrives på baggrund af systemelementernes output (hvor en "tilstand" også opfattes som et "output"). Ved systemdefinitionen skal der sørges for, at alle input og styrende signaler til systemet (funktionelle interaktioner såvel som øvrige påvirkninger af omgivelserne) er delt ud over de forskellige systemelementer (hvis hovedsystemet har et input, så må det input være input til mindst ét systemelement under hovedsystemet), og at alle output fra systemelementer har en "modtager" (enten et andet systemelement eller omgivelserne). På den måde er systemdefinitionen det direkte grundlag for fareidentifikationen.

Det skal bemærkes, at alle interaktioner og grænseflader betragtes: fx afskærmninger og vægge/døre/hegn tyder på en (mulig) interaktion med mennesker og et behov for at forhindre den interaktion.

Hvis der er flere niveauer af systemelementer (dvs. når hovedsystemets systemelementer igen er opdelt i mindre systemer), skal der vælges, på hvilket niveau HAZOP-metoden anvendes. At vælge et for detaljeret niveau (små systemelementer) skader ikke fareidentifikationen, men vil koste mange ressourcer, uden at fareidentifikationen behøver at blive væsentligt bedre. Systemelementer, som har et forholdsvis entydigt formål (dvs. output kan beskrives med få karakteristikker), og hvor der inde i selve systemelementet ikke med rimelighed kan forventes skadevoldende ulykker (fx inde i et el-skab eller motorkabinet) behøver ikke at blive opdelt i mindre systemer.

Eksemplet i anneks B3 af IEC vejledning 61882 stemmer i høj grad overens med beskrivelsen ovenfor. Eksemplet identificerer systemets interaktioner (input signal) og systemelementer (antenne, hastighedsmåler) med deres interaktioner (indgangs- eller udgangsspænding, hastighed, udgangssignal). Eksemplet medtager også "antennes position", som man efter ovenstående beskrivelse ikke vil "finde" som afvigelsen (men den vil være årsag til fx dårligt antennesignal), og det bemærkes også, at eksemplet ikke beskriver karakteristikkerne af systemelementernes interaktioner på en konsistent måde (for "Inputsignal" identificeres "Amplitude" og "Frekvens", mens der på systemelement-niveau ikke konsekvent identificeres interaktionen og dens karakteristikker).

4.3.1 Videre analyse af afvigelsen: konsekvenser

Ikke alle afvigelser genererer en fare i forhold til ulykker, som beskrevet i introduktionen, se afsnit 1. Det er derfor nødvendigt at vurdere de mulige konsekvenser af afvigelsen. Konsekvensen af en afvigelse findes typisk ved at stille spørgsmålet "hvad nu hvis <afvigelsen> sker?". Hvis der blandt deltagerne er enighed om, at afvigelsen ikke kan føre til en ulykke (se denne vejledning afsnit 2.1), behøver afvigelsen ikke at blive registreret i fareregistret. Det er vigtigt, at der i denne vurdering IKKE tages højde for allerede eksisterende eller forberedte sikkerhedsforanstaltninger, fordi sikkerhedsforanstaltninger betyder, at fraværet af risiko er på grund af disse tiltag, ikke fordi faren ikke er reel.

Når konsekvenser af afvigelser vurderes, skal det være på baggrund af mulige forværrende forhold, som med rimelighed må forventes at kunne forekomme, dog uden at tænke i helt ekstreme scenarier. Dette begrundes i, at CSM-forordningen taler om "potentielle" muligheder for ulykker[11]. "Potentiel" betyder at en situation muligvis, men ikke nødvendigvis, fører til en ulykke. Fx når et objekt kan falde ned på et område, som er tilgængeligt for personer, selvom det normalt ikke er befærdet, må det forventes, at det kan ramme en person. På den anden side, hvis en oversvømmelse kræver, at vandstanden i havet lokalt stiger med mere end 5 m højere end 1000-års bølgen, kan faren for oversvømmelse negligeres.

---

[11] CSM-RA-forordningen nr. 402/2013, som ændret ved gennemførelsesforordning 2015/1136 EU (European Commission, 2015), artikel 3, nr. 34) og Bilag I, punkt 2.5.8.

4.3.2 Årsager

Når der ved hjælp af kombinationen ”guideord” + ”karakteristik af interaktion” er genereret en meningsfuld mulig afvigelse i systemet, og det er vurderet, at der er tale om en reel fare, identificeres hvordan denne afvigelse kan opstå. Der kan være flere årsager til samme afvigelse. De skal hver registreres i fareregistret (på hver sin linje), da de hver kan give anledning til tiltag, som kan forebygge afvigelsen. Årsager skal søges i det systemelement, hvor afvigelsen har sin oprindelse, eller i påvirkningen af systemelementet fra omgivelserne.

Hvor ihærdig man skal være med at lede efter årsager, afhænger af muligheder for sikkerhedsforanstaltninger. Hvis faren kan kontrolleres ved at forhindre konsekvensen, uanset årsagen, er en komplet liste af årsager mindre relevant. Kan faren derimod kun kontrolleres ved at forhindre afvigelsen, skal man kunne kontrollere alle årsager, og så er det vigtigt, at alle årsager bliver identificerede.

4.3.3 Driftsforhold

Fareidentifikationen skal foretages for hver relevant driftsfase eller driftsforhold. Enten kan man dele fareidentifikationen op efter driftsfase (først analyseres operationel drift, bagefter vedligehold, osv.), eller man kan for hver afvigelse bestemme under hvilke driftsforhold, den medfører et problem: hvis der er flere (forskellige) konsekvenser og/eller årsager afhængigt af driftsforhold, tilføjes flere linjer i registret.

4.3.4 Registrering af afvigelser og farer

Som beskrevet i afsnit 2.5 anvender forskellige fareidentifikationsteknikker (lidt) forskellige tabelskabeloner for at registrere de identificerede farer. I denne vejledning foreslås en tabelskabelon for ”funktionsorienteret fareidentifikation ved hjælp af HAZOP-guideord”, som er baseret på en skabelon fra IEC’s HAZOP-vejledning (IEC, 2001), se Tabel 2. Ændringen i skabelonen er, at overskriftsdelen er tilpasset CSM-RA og brug af ”systemelement”-begrebet, hvor interaktionerne bruges til at generere afvigelser. Ændringen i tabellen er tilføjelse af kolonnen ”Driftsforhold” for at håndtere driftsforhold som beskrevet i afsnit 4.3.3 ovenfor.

I første del af overskriften registreres projekt, baggrundsmateriale, dato og øvrige administrative detaljer, som er nødvendige for at dokumentere, at fareidentifikationsprocessen er gennemført ordentligt.

I anden del af overskriften registreres detaljerne for den pågældende side af tabellen: der laves i det mindste en ny tabel for hvert systemelement; det kan også vælges efterfølgende at lave en ny tabel for hvert driftsforhold (se afsnit 4.3.3) og/eller for hver interaktion eller interaktionskarakteristik: det afhænger af, hvor omfattende og komplekse systemelementerne er, eller hvor forskellige driftsforholdene er. Når samme tabel dækker forskellige driftsforhold, skal det fremgå af overskriften (fortrinsvis ved at liste alle relevante driftsforhold, som er vurderede, i stedet for at skrive ”alle driftsforhold”), og når tabellen dækker over forskellige interaktioner, skal disse listes i overskriften, som vist i Tabel 2.

I den nederste del registreres de identificerede afvigelser. Følgende skal registreres i kolonnerne:

- *Ref. Nr.*: Hver afvigelse eller fare gives et unikt nummer eller kode, som kan overføres til projektets fareregister;
- *Guideord*: Her gentages det guideord, som er anvendt til at generere afvigelsen med, fx ”mere”;
- Interaktionens karakteristik: Her gentages den karakteristik, som er anvendt til at generere afvigelsen med, fx ”bremserørets lufttryk”;
- *Afvigelse*: Her formuleres den konkrete afvigelse på sådan en måde, at den giver mening i systemet, fx ”bremserørets tryk er højere end 5,5 bar”;

- *Driftsforhold*: Hvis ikke driftsforhold er defineret i tabellens overskrift, skrives driftsforhold her. Det kan omfatte flere situationer, hvis afvigelsen er relevant og har samme betydning for disse situationer, fx: ”kørsel og standsning ved stationer”;
- *Mulige årsager*: Her skrives de mulig årsager til afvigelsen. Hvis der er flere årsager, og disse årsager kan kontrolleres ved forskellige sikkerhedsforanstaltninger, tilføjes nye linjer. Det er ikke nødvendigt at gentage indhold i de øvrige kolonner, hvis det er tydeligt, hvilken afvigelse årsagerne hører til. Der tilføjes sikkerhedsforanstaltninger til linjen, hvis foranstaltningen (kun) vedrører årsagen på linjen;
- *Mulige konsekvenser*: her skrives, hvilke konsekvenser afvigelsen kan få, som i de fleste tilfælde vil skrives som en ulykke med ulykkens konsekvenser (se listen med forordningens ulykkestyper i introduktionen - afsnit 1 – og/eller ved at nævne alvorligheden, som personskade, materielle skader, dødsfald, o.l.);
- *Sikkerhedsforanstaltninger*: Her skrives, hvilke sikkerhedsforanstaltninger der er truffet (eksisterende) eller kan træffes (til overvejelse eller anbefaling). Status (eksisterende/planlagt/til overvejelse) inkluderes i beskrivelsen. Sikkerhedsforanstaltninger kan vedrøre konsekvenser (afværgende tiltag som forhindrer, at afvigelsen fører til ulykker, eller som vil mindske konsekvens af ulykker) eller årsager (foranstaltninger som forebygger afvigelsen). Der kan tilføjes nye linjer for at tydeliggøre dette;
- *Bemærkninger*: Dette felt kan bruges efter behov. Det kan fx skrives her, hvis der er uenighed eller usikkerhed blandt deltagerne om nogle forhold;
- *Aftalte aktioner*: Her skrives aktioner i forhold til de registrerede afvigelser, årsager eller sikkerhedsforanstaltninger. Det kan fx være, at der er forhold som skal afklares, så som specifikationer for eksisterende sikkerhedsforanstaltninger;
- *Ansvarlig for aktion*: Når der er aftalt en aktion, skal én af deltagerne tage ansvar for, at aktionen gennemføres.

4.4 Fordele og ulemper ved funktionsorienteret metode ved hjælp af HAZOP-guideord

4.4.1 Fordele

- Systematisk, struktureret og i dybden;
- Kræver interaktion og bidrag fra eksperter på tværs af fagområder;
- Kan anvendes på mange forskellige typer af systemer (herunder også organisatoriske systemer og procedurer som i IEC 61882 anneks 3B);
- Kan anvendes på innovative systemer (ingen referencer med tidligere erfaringer er nødvendige);
- Resultatet og dokumentationen kan auditeres med henblik på at vurdere kvaliteten af processen.

4.4.2 Ulemper

- Kræver betydelig forberedelse;
- Ressource- og tidskrævende;
- Kræver en ordstyrer med erfaring i HAZOP
- Kan forhindre kreativ tænkning og identifikation af farer udover dem, som kan genereres ved guideord teknikken.
- Resultatet er i høj grad afhængigt af kvaliteten af systemdefinitionen: funktioner, grænseflader og interaktioner, som ikke er identificerede i systemdefinitionen, vil ikke kunne generere afvigelser.

Tabel 3 Forslag til tabelskabelon som kan bruges til at registrere afvigelser genereret ved hjælp af HAZOP-guideord

Funktionsorienteret fareidentifikation ved hjælp af HAZOP-guideord				**Tabel**	1 af …
Projekt:				**Møde dato:**	(dato)
Systemdefinition:		**Revision nr:**		**Renskrevet:**	(dato)
Evt. bilag:		**Revision nr:**		**Revideret:**	(dato)
Deltagere:					
Systemelement:	*fx Integrated Relay Valve i IC4 bremsesystem*				
Systemelementets funktion:	*At regulere tryk til bogiens bremsecylindre*				
Driftsforhold:	*(fx "kørsel", kan også håndteres i tabellen)*				

Interaktion	**Karakteristik:**	**Kommer fra:**	**Går til:**
fx input: pneumatisk tryk	*Fx lufttryk*	*Fx hovedrør (auxiliary reservoir)*	*(dette systemelement)*
fx kontrol: tryk i bremserøret	*Fx lufttryk*	*Fx bremserør (service brake pilot)*	*(dette systemelement)*
fx output: tryk til bremsecylindre	*Fx lufttryk*	*(dette systemelement)*	*Fx bremsecylindre via WSP dump valves*

Ref. nr.	**Guideord**	**Interaktionens karakteristik**	**Afvigelse**	**Driftsforhold**	**Mulige årsager**	**Mulige konse-kvenser**	**Sikkerheds-foranstaltninger**	**Bemærk-ninger**	**Aftalte akti-oner**	**Ansvarlig for aktion**
1										
2										
3										
4										
5										

5. Metode 2: FMEA/FMECA

Failure Mode and Effect Analysis (FMEA) blev introduceret mellem 1940 og 1950 i det amerikanske forsvar, og senere anvendt i luft- og rumfart for at forhindre fejl i produktion af små serier af kostbart udstyr. FMEA anvendes i dag i vid udstrækning i udvikling af komplekse teknologiske systemer (fx medicinsk udstyr), såvel som mere enkle forbrugsprodukter. Det er en anerkendt metode i processen til at demonstrere overensstemmelse med CE-maskindirektivet og lignede forskrifter.

FMEA er en induktiv eller "bottom-up" metode, som har fokus på komponenter og opdeling af systemer i små, enkle enheder. Metoden går ud på at identificere alle mulige måder, hvorpå disse små elementer eller komponenter kan fejle på, og så vurdere hvordan disse fejl påvirker det større system. Forud for FMEA skal systemet nedbrydes i et hierarki af mindre delelementer. I princippet skal det nedbrydes til skruer og møtrikker, men i praksis nøjes man med at nedbryde til et niveau af delelementer, hvor man mener at have tilstrækkelig forståelse for den måde, disse delelementer kan fejle på.

FMECA, Failure Mode, Effect and Criticality Analysis, er en udvidelse af FMEA, hvor der i processen laves en vurdering af, hvor kritisk fejlen er, med henblik på at kunne prioritere de vigtigste fejl. Det opnås ved at kombinere et mål for de mulige konsekvensers alvor med fejlens sandsynlighed i en måleenhed som kaldes kritikalitet.

FMEA og FMECA er beskrevet i IEC standard 60812 (IEC, 2006). Relevante afsnit er kapitel 3 (termer og definitioner); kapitel 4; afsnittene 5.1, 5.2, og 5.3 (for FMECA) og Anneks A. Nyttige oplysninger og eksempler findes i afsnit 5.4; kapitlerne 6 og 7 og Anneks B. Beskrivelsen gentages ikke her.

Til anvendelse af FMEA/FMECA skal systemdefinitionen indeholde følgende oplysninger:

- Beskrivelse af alle systemelementer med funktion, opbygning og specifikationer;
- (Logiske) interaktioner mellem elementerne
- Beskrivelse af redundans
- Interaktion af systemet med dets omgivelse, herunder input og output
- Ændringer i systemets opbygning under forskellige driftsforhold.

5.1 Detaljeniveau i FMEA

Udfordringen ved FMEA er håndtering og valg af detaljeniveau. Deler man systemet op i enkelte komponenter, er der et begrænset antal basale fejlmuligheder, men antallet af komponenter, som skal vurderes, bliver stort. Hvis systemet derimod deles op i større og dermed lidt mere komplekse delelementer, er der færre enheder, som skal gennemgås. Men det antal basale fejlmuligheder af disse delelementer vil være lidt større og muligvis vanskeligere at bestemme.

Også små komponenter kan allerede have et betydeligt antal basale fejlmuligheder; der henvises til (CENELEC, 2003), Anneks C, som indeholder basale fejlmuligheder for en række elektriske og elektroniske komponenter. Fx har en enkel bipolar transistor som udgangspunkt 19 basale fejlmuligheder. En FMEA kan eventuelt sammensættes ved hjælp af en FMEA gennemført for enkelte delelementer. Fx kan en FMEA for et system hvor der indgår forskellige elektroniske kredsløb, bygge videre på de FMEA, som er udført for de enkelte kredsløb, fx af leverandøren af disse kredsløb.

5.2 Dokumentation af FMEA workshop

Det anbefales, at en FMEA/FMECA udføres ved hjælp af en workshop med et team af eksperter. Det er dog muligt, at en del af arbejdet, fx at identificere de basale fejlmuligheder for kendte komponenter, forberedes af

en enkel sagkyndig. Teamets bidrag er størst ved en diskussion om, hvordan de enkelte fejl forplantes gennem systemet og kan føre til relevante farer.

Kvaliteten af FMEA afhænger bl.a. af, om man anvender udtømmende lister af basale fejlmåder for de enkelte komponenter, som indgår i analysen. Det anbefales for hver (type af) komponent, at sådan en liste inkluderes i dokumentationen af FMEA (i lighed med (CENELEC, 2003), Anneks C).

Resultater af en FMEA dokumenteres i tabelformat, en skabelon er inkluderet i standarder, som kan overføres til et regneark. Der findes også frie og kommercielle software-værktøjer for at støtte og dokumentere FMEA's og FMECA's analyser (PHA Pro, ReliaSoft, og mange flere). Tabel 3 viser et forslag til, hvordan en tabel til FMEA i CSM-RA kan se ud.

I første del af overskriften registreres projekt, baggrundsmateriale, dato og øvrige administrative detaljer, som er nødvendige for at dokumentere, at fareidentifikationsprocessen er gennemført ordentligt.

I anden del af overskriften registreres detaljerne for den pågældende side af tabellen. I hvert tilfælde angives hovedsystemet, som i FMEA sammenhæng betyder det system, man til sidst vil vurdere effekten af fejl på. Det behøver ikke at være hele projektets hovedsystem som defineret i systemdefinitionen, men kan være et (større) systemelement. Hovedsystemet opdeles i små delelementer eller komponenter. Man kan vælge enten at lave en tabel for hver komponent, eller at samle flere komponenter (hvis de er enkle og har få basale fejlmåder) i én tabel. Afhængig af valget tilføjes oplysninger om komponent (eller "emne") i tabellens overskrift.

I den nederste del registreres de forskellige fejlmåder og deres mulige konsekvenser. Følgende skal registreres i kolonnerne:

- *Emneref.*: Hvis der vælges, at tabellen omfatter flere emner (komponenter), identificeres emnet i denne kolonne;
- *Emne: beskrivelse og funktion*: Hvis der vælges, at tabellen omfatter flere emner, beskrives emnet og dets funktion;
- *Fejlmåde*: Her beskrives de basale måder hvorpå emnet (komponenten) kan fejle på. Fx for en møtrik: "*Løs; Løs, kan ikke strammes; Fast med for høj moment; Fast, kan ikke løsnes; Brudt*". For mere inspiration vedr. basale fejlmuligheder, se (CENELEC, 2003), Anneks C;
- *Fejlkode*: Hver fejl eller fare gives et unikt nummer eller kode, som kan overføres til projektets fareregister. Ved FMEA kan fejlkoden bestå af emnereferencen plus en kode for en specifik basal fejlmulighed;
- *Mulig fejlårsag*: Her skrives de mulige årsager til den basale fejlmåde. Da FMEA identificerer fejl på et lavt niveau, plejer man ikke at tilføje en ny linje (med en ny unik fejlkode) for flere årsager, men hvis man ønsker at kunne følge en bestemt årsag (med eventuelle forebyggende foranstaltninger) gennem fareregistret, skal der tilføjes en ny linje;
- *Lokal effekt*: Den lokale effekt beskriver, hvilke følger den basale fejlmåde har for komponenten og komponenter i den umiddelbare nærhed eller det delelement på næsthøjeste niveau, hvori komponenten indgår. Fx betyder en løs møtrik, at nogle dele ikke kan holdes samlet;
- *Sluteffekt*: Sluteffekten er den effekt, som fejlen kan have på det system, der i FMEA er defineret som hovedsystem. Det er konsekvensen af den lokale effekt på det højeste niveau i FMEA. Sluteffekten skal i CSM-RA sammenhæng relateres til mulighed for en ulykke (se listen med jernbanesikkerhedsdirektivets ulykkestyper i afsnit 1-Introduktion) og ulykkens konsekvenser som personskade, materielle skader, dødsfald, o.l.;
- *Fejldetektering, metode og mulighed*: I FMEA vurderes, om der er muligheder for at detektere den basale fejl (inden den fører til ulykker). Det kan være pga. aktiv overvågning (fx i elektriske eller elektroniske

kredsløb) eller ved regelmæssig inspektion. Fejldetektering kan opfattes som en særlig form for sikkerhedsforanstaltninger som FMEA har særligt fokus på;

- *Foranstaltninger mod fejl:* Her skrives hvilke sikkerhedsforanstaltninger der er truffet (eksisterende) eller kan træffes (til overvejelse eller anbefaling). Status (eksisterende/planlagt/til overvejelse) inkluderes i beskrivelsen. Sikkerhedsforanstaltninger kan vedrøre konsekvenser (afværgende tiltag som forhindrer at fejlen fører til uheld, eller som vil mindske konsekvenserne af en ulykke) eller årsager (foranstaltninger som forebygger fejlen);
- *Alvorlighed: I FMEA tilføjes ofte en vurdering af fejlens alvorlighed, eller alvorligheden af den mulige konsekvens af fejlen. Det skal angives, om alvorligheden allerede har taget (eksisterende) afværgende foranstaltninger i betragtning. Der kan med fordel henvises til CSM-forordningens definition af katastrofal og kritisk ulykke12;*
- *Fejlfrekvens eller fejlsandsynlighed: Ligesom alvorlighed: Der kan tilføjes en vurdering af sandsynligheden for fejl. Det skal angives, om sandsynligheden allerede har taget (eksisterende) forebyggende foranstaltninger i betragtning;*
- *Bemærkninger: Dette felt kan bruges efter behov. Det kan fx skrives her, hvis der er uenighed eller usikkerhed blandt deltagerne om nogle forhold. Dette felt kan også bruges til at tilføje aftalte aktioner, hvis der ikke bruges særlige kolonner dertil som i HAZOP tabellen (Tabel 2).*

[12] CSM-RA-forordningen nr. 402/2013, som ændret ved Ggennemførelsesforordning 2015/1136 EU (European Commission, 2015), artikel 3, nr. 23) og 35).

Tabel 4 Forslag til tabelskabelon som kan bruges til at registrere fejlmuligheder genereret ved hjælp af FMEA

FMEA worksheet (baseret på IEC 60812, Annex A)				**Tabel**	1 af …
Projekt:				**Møde dato:**	(dato)
Systemdefinition:		**Revision nr:**		**Renskrevet:**	(dato)
Evt. bilag:		**Revision nr:**		**Revideret:**	(dato)
Deltagere:					
Hovedsystem (sluteffekt):	*fx IC4 Bremsesystem*				
Emne/Komponent:	*fx Relaisventil "R" i IRV (Integrated Relay Valve)*				
Emneref.:		**Referencedokument for komponent:**		**Revision nr:**	
Driftstilstand:	*fx pneumatisk bremsekommando 4 bar*				

Emne-ref.	Emne: beskrivelse og funktion	Fejlmåde	Fejl kode	Mulige fejlår-sager	Lokal effekt	Sluteffekt (Ho-vedsystem)	Fejldetektering, metode og mu-lighed	Foranstalt-ninger mod fejl	Alvorlighed	Fejlfrekvens el-ler sandsynlig-hed	Bemærkninger

5.3 Fordele og ulemper ved FMEA og FMECA

5.3.1 Fordele

- Systematisk, struktureret og i dybden;
- Kan anvendes på innovative systemer (ingen referencer med tidligere erfaringer er nødvendige);
- Kan anvendes på alle tekniske systemer og kan eventuelt også anvendes på organisatoriske systemer og andre systemer i forhold til drift;
- Resultatet og dokumentationen kan auditeres med henblik på at vurdere kvaliteten af processen.

5.3.2 Ulemper

- Ressource- og tidskrævende;
- Kræver indgående og detaljeret kendskab til systemet af alle deltagere
- Kræver en udtømmende forståelse af basale fejlmuligheder
- Identificerer kun fejl som følge af komponentfejl - det kan forhindre identifikation af fejl som opstår på grund af interaktion mellem komponenterne (fx i organisatoriske systemer);

6. Metode 3: Tjeklister

6.1 Generelle tjeklistemetoder

Tjeklister opfattes ofte som en forholdsvis nem metode til at identificere farer på. Fremgangsmåden består i, at en liste med farer eller potentielt farlige forhold gennemgås systematisk, og at der for hvert emne på listen tages stilling til, om den fare, eller en lignende fare, er relevant for det system som bliver vurderet.

Metoden er struktureret ved, at listen afvikles systematisk. Om man får alle farer identificeret afhænger af, om tjeklisten er udtømmende for den type system som bliver vurderet.

Tjeklistemetoder anvendes oftest på hele systemer snarere end på systemelementer. Metoden genererer derfor sjældent farer på et detaljeret niveau. Det kan ved større systemer være en fordel at dele systemet op i nogle delelementer, hvis de har klart forskellige funktioner eller grænseflader. Sådan en opdeling vil kunne være i lighed med den, som man vil anvende for et HAZOP-studie, se afsnit 5.1.

Der kan differentieres mellem to typer af tjeklister.

Den første type tjeklister formulerer farer eller afvigelser direkte, muligvis på et overordnet niveau, se Bilag A, fx Tabel A 1 og Tabel A 2. Teamets opgave er at finde ud af om de nævnte farer er relevante for systemet, og hvis ja, at specificere faren tilrettet det pågældende system (fx under hvilke driftsforhold eller på hvilke områder), og at identificere årsager og konsekvenser.

Den anden type tjeklister indeholder kun emneord for generiske områder eller faktorer, som ikke direkte kan opfattes som farer. Teamets opgave er at generere og formulere farer, som er relevante for disse emner. Det gøres bedst ved at formulere emnerne som spørgsmål, fx:

- ”Afsporing”: Kan (eller ”hvordan kan”) dette system føre til afsporing?
- ”Jernbaneovergang”: Hvilke farer er forbundne med jernbaneovergangen?
- ”Vedligehold”: Hvad nu hvis vedligehold ikke udføres korrekte?

Disse tre emner er taget fra tjeklisten, som er inkluderet i (CENELEC, 2007); listen er inkluderet i Tabel A 3. Disse tre emner viser, at der ikke er én måde at formulere spørgsmålene på. Særlige måder at stille spørgsmålet på er ”Hvad nu hvis …” (What if …) eller ”hvordan kan …” (How can …). ”What-if”-metoden eller SWIFT (Structured What IF Technique) anses ofte for at være en særlig fareidentifikationsteknik, se afsnit 6.2.

Ovenstående viser, at den anden type af tjeklister er sværere at håndtere og kræver en nærmere bestemt struktur (fx SWIFT, se afsnit 6.2) for den måde, man genererer farer ud fra tjeklisternes emner. Den første type af tjekliste er derfor nemmere at håndtere, og metoden er også nemmere at dokumentere.

6.2 “What-if” teknikker (SWIFT)

SWIFT er oprindeligt udviklet som et nemmere og hurtigere alternativ til HAZOP, hvor man på et højere niveau (færre systemelementer) fremprovokerer afvigelser ved færre og mere åbne spørgsmål (What if: Hvad nu hvis …?; Hvordan kan …?; Har man nogensinde…?). SWIFT kræver dog, at man har en række emner, som man anvender spørgsmålene på, og derfor beskrives metoden her under ”tjeklister”. SWIFT kræver, at ordstyreren (eller den person som har ansvar

for fareidentifikationen) forbereder en liste med emner, som er relevante for systemet, og som bliver brugt som inspiration til identifikation af farer. Emnerne kan enten være karakteristikker af systemet, omgivelserne eller driftsforhold (fx dem som er vist i Tabel A 3) eller relevante ulykkestyper. Dokumentation af fareidentifikationen ved hjælp af SWIFT bør omfatte emnelisten, som er anvendt, og en (kort) beskrivelse af identifikationsprocessen (spørgsmål) udover kraavene beskrevet i kapitel 2.

6.2.1 Fordele og ulemper ved SWIFT:

1.1.1.1 Fordele

- Mindre tidskrævende end HAZOP og FMEA;
- Resultatet og dokumentationen kan auditeres med henblik på at vurdere kvaliteten af processen.

1.1.1.2 Ulemper

- Resultat er afhængigt af emnelistens kvalitet
- Resultatet er afhængigt af ekspertisen af deltagerne og ordstyreren.

6.3 Udtømmende tjeklister

Den store udfordring ved tjeklister er, at de med rimelighed skal være udtømmende for den type system som skal vurderes, dvs. tjeklisten skal repræsentere "alle tilgængelige oplysninger[13]", som vedrører dette system. En generisk tjekliste, som dækker alle (jernbane)systemer er formodentligt for ambitiøst og vil også blive så lang, at det ikke længere er praktisk, og fordelen med tjeklisten vil gå tabt. En del af udfordringen består derfor i at vælge den rigtige tjekliste. For at det kan sikres, at fareidentifikationen ved hjælp af tjeklister er struktureret (se krav i introduktionen, kapitel 1) skal der kunne argumenteres for, at den anvendte tjekliste dækker alle farer som med rimelighed kan forventes at kunne opstå i forbindelse med det pågældende system.

I almindelighed er proceduren, at man finder en eksisterende tjekliste, og at man tilpasser tjeklisten baseret på både observerede hændelser (se afsnit 2.1) og fareidentifikationen ved hjælp af ikke-tjekliste-baserede (dvs. HAZOP- eller FMEA-lignende) teknikker. For at sikre at tjeklisten er nogenlunde udtømmende, skal man gennemgå flere (i størrelsesorden mindst 5) fareidentifikationer for samme type system, for at se, om der mangler emner.

I Bilag A til vejledningen er der vedlagt nogle eksempler på tjeklister.

RSSB (RSSB, 2014) præsenterer et eksempel på en tjekliste for rullende materiel, som ikke må opfattes som udtømmende. Denne tjekliste er efter en mindre bearbejdning (listen er blevet emneinddelt, og der er tilføjet nogle elementer under "infrastruktur") vedlagt i Bilag A, Tabel A 1.

Tabel A 2 præsenterer en liste over mulige arbejdsulykker. Den er baseret på en gennemgang af flere tusinde registrerede arbejdsulykker, og det kan siges, at alle observerede arbejdsulyk-

[13] CSM-RA-forordningen, artikel 3, nr. 2: definition af risikoanalyse: systematisk anvendelse af alle tilgængelige oplysninger til at identificere farer og estimere risikoen

ker kan indordnes i denne liste, så den må opfattes som værende udtømmende for almindelige arbejdsulykker, se (Jørgensen, Duijm, & Troen, 2010). Den vil også kunne bruges til at identificere farer for passagerer og tredjepart i nærheden af almindelige arbejdspladser. Den omfatter dog ikke farer for jernbanesystemet som sådan (infrastruktur eller rullende materiel).

CENELEC's vejledning til EN 50126 (CENELEC, 2007) beskriver fareidentifikation ved hjælp af tjeklister, og den indeholder i bilag B forskellige tjeklister. I Tabel A 3 er én af listerne vedlagt, hvor emnerne er aspekter, som kan medføre farer (dvs. man skal generere farer ved at udforske emnerne nærmere ved hjælp af spørgsmål, se 6.1). CENELEC anbefaler, at man altid sikrer, at tjeklisten er dækkende for det system, som skal vurderes, så de præsenterede lister er ikke nødvendigvis udtømmende. Det betyder, at hvis man vil anvende disse tjeklister, er det nødvendigt at gennemgå nogle (i størrelsesorden mindst 5, se ovenfor) lignende fareidentifikationer, som er baseret på mere grundlæggende metoder (HAZOP, FMEA eller lignende) for at sikre, at tjeklisten med rimelighed er udtømmende.

6.4 Dokumentation af tjeklistemetoden.

Der findes ikke en standard eller standardbeskrivelse af tjeklistemetoden. Til dokumentation kan bruges almindelige regneark. Nogle af de tidligere nævnte softwareværktøjer kan også bruges til tjekliste-lignende metoder (fx SWIFT). Tabellens overskift kan være i lighed med overskriften til FMEA tabellen. Tabellen skal helst indeholde de følgende kolonner:

- Kolonne til et identifikationsnummer
- Systemelement, hvis systemet er analyseret per delelement
- Emneordet fra tjeklisten
- Specificeret beskrivelse af fare for det pågældende system
- Driftsforhold
- Mulige årsager til faren
- Mulige konsekvenser af faren
- Risikoreducerende tiltag
- Eventuelle bemærkninger
- Aftalte aktioner
- Ansvarlig for aktion

Rapportering af fareidentifikationsprocessen ved hjælp af en tjekliste skal indeholde den fulde tjekliste, som er anvendt. Sammen med kolonnen "Emneord" er en assessor i stand til at vurdere systematikken i fareidentifikationen. I dokumentationen bør der redegøres for, hvorfor man mener, at tjeklisten er udtømmende (fx ved henvisning til kilden og gennemgang af andre fareidentifikationer).

Modsat HAZOP og FMEA/FMECA er der for tjeklistemetoden ikke en foreskreven måde at dele systemet op i mindre delelementer. Dokumentationen bør indeholde en beskrivelse af, hvordan denne opdeling er gennemført, hvis det har været tilfældet.

6.5 Fordele og ulemper med generelle tjeklistemetoder

6.5.1 Fordele

- Kan gennemføres indenfor rimelig tid;
- Kræver ikke indgående kendskab til fareidentifikationsmetoder;

- Tjeklister kan rumme et stort omfang af viden og tidligere erfaringer;
- Usandsynligt at almindelige og mere åbenlyse farer overses.

6.5.2 Ulemper

- Bør ikke anvendes på innovative systemer, hvor der ikke er tilstrækkelig erfaring;
- Kvaliteten er afhængig af kvaliteten af tjeklisten;
- Kan forhindre kreativ tænkning og identifikation af farer udover dem, som er omfattet af tjeklisten;
- Det er sandsynligt, at farer som ikke er observeret før, vil blive overset.

7. Metode 4: Genbrug af tidligere fareidentifikationer

Der vil være mange situationer, hvor systemer eller systemændringer ligner hinanden, og det er nærliggende, at man genbruger fareidentifikationen fra tidligere, lignende projekter.

Der er to måder at genbruge en eksisterende fareidentifikation på:

1. Farer fra en (eller flere) tidligere fareidentifikation(er) generaliseres til en tjekliste, og tjeklisten bruges som beskrevet i kapitel 6, med alle dertilhørende fordele, ulemper og udfordringer (herunder for at demonstrere at tjeklisten er udtømmende);
2. Fareidentifikationen kopieres som sådan.

Fremgangsmåden under ovenstående punkt 2. er ikke en praksis, som beskrives i litteraturen, men den har nogle åbenlyse fordele i, at den genbruger viden og dermed sparer ressourcer som delvist kan bruges til at forbedre kvaliteten af risikostyringsprocessen. En anvendelse af genbrugsmetoden på jernbaneområdet beskrives i (Winther, 2015). EPSC's HAZOP vejledning (Crawley et al., 2000) nævner "HAZOP by difference" som metode til at identificere farer i systemer som er næsten identiske, men metoden beskrives ikke nærmere.

Fremgangsmåden under punkt 2. er kun acceptabel, hvis den kopierede fareidentifikation er grundlag for en gennemgang i fareidentifikationsworkshoppen. Gennemgangen deles op i to:

- Der tages stilling til, om hver af de kopierede farer (stadig) er relevante for det nye projekt. Beskrivelserne tilpasses til det nye projekt – disse ændringer markeres i kolonnen "bemærkninger" (eller en tilsvarende kolonne) i tabellen, for at assessoren kan følge processen.
- Der laves en nøje sammenligning mellem det tidligere projekts systemdefinition og det nye projekts systemdefinition. Relevante forskelle[14] dokumenteres, og teamet vurderer, om disse forskelle fører til nye farer (eller nye årsager hhv. konsekvenser for allerede identificerede farer) ved hjælp af én af de tidligere beskrevne teknikker i afsnit 4 til og med 6. Det kan også være, at der er nogle farer i den tidligere liste, som kan fjernes for det nye projekt. Disse ændringer indarbejdes i farelisten for det tidligere projekt, som nu er farelisten for det nye projekt.

Eventuelle erfaringer fra det tidligere projekt (ikke-identificerede farer som er fremkommet efterfølgende) bør selvfølgelig også tilføjes.

Dokumentationen bør indeholde:

- En kort beskrivelse af fareidentifikationsprocessen (i stil med beskrivelsen ovenfor);
- En redegørelse for, hvorfor man mener, at det tideligere projekts fareidentifikation kan genbruges;
- En liste med forskelle mellem systemerne, som er vurderet mht. nye/udvidede farebeskrivelser.

---

[14] Relevante forskelle kan være, at nogle grænseflader og interaktioner er af en anden art; at der er væsentlige forskelle i specifikationer af interaktioner, (del)systemer, antagelser, osv.. Ikke-relevante forskelle er forskelle som ikke kan forventes at påvirke systemets virke, fx geografisk lokalitet som sådan – medmindre det medfører andre omgivelsespåvirkninger (fx mulighed for oversvømmelse).

- Farelisten for det nye projekt, hvori ændringer i forhold til den oprindelige fareliste for det tidligere projekt er markeret og redegjort;
- Systemdefinitionen for både det tidligere og det nye system skal være tilgængelig (for assessoren).

7.1 Fordele og ulemper mht. til ”genbrug”

7.1.1 Fordele

- Mindre tidsforbrug ved udnyttelse af tidligere arbejde;
- Bygger videre på eksisterende viden og tidligere erfaringer;
- Fokus på ændringer i systemet, og dermed bedre udnyttelse af deltagerne.

7.1.2 Ulemper

- Kan kun anvendes, når der findes et tidligere projekt, som ligner det nye projekt i høj grad;
- Kan forhindre kreativ tænkning og identifikation af farer udover dem, som allerede er identificeret;
- Meget sandsynligt, at farer, som ikke er observeret før, vil blive overset.

8. Anvendelse på organisationer eller procedurer

De præsenterede fareidentifikationsmetoder kan uden de store problemer anvendes både på organisatoriske ændringer og ændringer i driftsprocedurer, hvis systemdefinitionen indeholder en klar beskrivelse af disse ændringer i termer af ansvar, opgaver, formål, grænseflader og interaktioner (kommunikation). Der henvises til vejledning om systemdefinition, som redegør for at ændringer i drift enten er ændringer i driftsprocedurer eller vedrører organisatoriske eller tekniske forhold.

8.1 Organisatoriske ændringer

Ved organisatoriske ændringer vil fareidentifikationen fokusere på:

- Om de nødvendige ressourcer (mht. antal, kompetence og egnethed) vil være til rådighed for at udføre opgaver, som er nødvendige for at kontrollere farer;
- Om der kan opstå konflikter mellem opgaver, som gør, at aktiviteter, der er nødvendige for at kontrollere farer, bliver nedprioriteret (på niveau af den enkelte medarbejder eller på de forskellige ledelsesniveauer);
- Om organisationen medvirker til, at medarbejderne har adgang til information og kan udføre den kommunikation, der er nødvendig for at kontrollere farer;
- Om den enkelte medarbejder får tilstrækkelig støtte og har tilstrækkelig autoritet til at udføre sine opgaver, som er nødvendige for at kontrollere farer.

8.2 Ændringer i driftsprocedurer

Ved ændringer i procedurer bør systemdefinitionen omfatte en opgaveanalyse (task analysis). En opgaveanalyse er en analyse af, hvordan en opgave udføres, herunder en detaljeret beskrivelse af:

- manuelle og mentale aktiviteter,
- varighed af opgaven og dens aktiviteter,
- opgavens frekvens,
- opgavefordeling,
- opgavens kompleksitet,
- miljøforhold,
- nødvendigt tøj og udstyr,
- eventuelle andre unikke faktorer involveret i eller som kræves for, at en eller flere personer kan udføre opgaven.

Sådan en opgaveanalyse vil danne grundlag for en fareidentifikation ved enten HAZOP (med fokus på formål og resultater af opgaven og aktiviteter), FMEA (med fokus på om de enkelte delaktiviteter udføres korrekte, og hvordan fejl vil påvirke opgavens resultat) eller ved hjælp af tjeklister.

IEC vejledning 61882 (vedr. HAZOP) indeholder i dens anneks B2 et eksempel af anvendelse af HAZOP metoden på en procedure.

Referencer

CENELEC. (2003). Railway applications - communication, signalling and processing systems - safety related electronic systems for signalling. (European Standard No. EN 50129). Brussels: CENELEC.

CENELEC. (2007). *Railway applications - the specification and demonstration of reliability, availability, maintainability and safety (RAMS) - part 2: Guide to the application of EN 50126-1 for safety.* (Technical report No. CLC TR 50126-2:2007). Brussels: CENELEC.

Crawley, F., Preston, M., & Tyler, B. (2000). *HAZOP guide to best practice - guidelines to best practice for the process and chemical industries*. Rugby, UK: IChemE/EPSC.

DTA. (2010). *Vejledning i anvendelse af helhedsorienteret risikovurdering - ved infrastrukturprojekter og tekniske regler for infrastruktur.* (). Copenhagen: Trafikstyrelsen/Danish Transport Authority.

European Commission. (2004). *"Railway safety directive".* (No. 004/49/EC). Luxembourg: Publications Office of the European Union. . (Official Journal of the European Union L 164 of 30 April 2004)

European Commission. (2013). *Regulation on the common safety method for risk evaluation and assessment.* (Regulation from the European Commission No. 402/2013/EC). Luxembourg: Publications Office of the European Union. doi:10.3000/19770677.L_2013.121.eng

European Commission. (2015). *COMMISSION IMPLEMENTING REGULATION (EU) 2015/1136 of 13 july 2015 amending implementing regulation (EU) no 402/2013 on the common safety method for risk evaluation and assessment.* (Regulation from the European Commission No. 2015/1136/EC). Luxembourg: Publication Office of the European Union.

IEC. (2001). *Hazard and operability studies (HAZOP studies) - application guide, IEC 61882:2001.* (No. IEC 61882).IEC.

IEC. (2006). *Analysis techniques for system reliability - procedure for failure mode and effect analysis (FMEA).* (No. IEC 60812:2006(E)). Brussels: CENELEC.

Jørgensen, K., Duijm, N. J., & Troen, H. (2010). *Risikovurdering og forebyggelse af arbejdsulykker.* ().DTU Management.

Jovicic, D. (2009). *Guide for the application of the commission regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in article 6(3)(a) of the railway safety directive.* (No. ERA/GUI/01-2008/SAF, version 1.1).European Railway Agency.

Kletz, T. (1999). *Hazop and hazan - identifying and assessing process industry hazards* (4th ed.). Rugby, UK: IChemE.

ORR. (2015). Common safety method for risk evaluation and assessment - guidance on the application of commission regulation (EU) 402/2013. (). London: Office of Rail Regulation, UK.

RSSB. (2014). *Guidance on hazard identification and classification.* (No. GE/GN8642, Issue Two). London: Rail Safety and Standards Board Limited.

Winther, R. (2015). A pragmatic approach to the reuse of qualitative risk and reliability analyses—experiences from analyses of railway traction substations. *ESREL Safety and Reliability of Complex Engineered Systems,* Zürich. 3681-3689.

Bilag A Eksempler på tjeklister

RSSB (RSSB, 2014) beskriver forskellige fareidentifikationsmetoder, herunder brug af tjeklister. Der introduceres et eksempel for "rullende materiel", som ikke er udtømmende. Listen er, efter emneinddeling i forhold til faretypen eller hændelsen, gengivet i nedenstående tabel. Emnerne er præsenteret som den skadeforvoldende hændelse (ulykke).

Tabel A 1 Tjekliste baseret på eksempel i Rullende materiel CSSB (RSSB, 2014), ordnet; ikke udtømmende (præsenteret som eksempel for rullende materiel)

3rd party hazards/passengers outside train	Insufficient warning of presence of train Potential for train surfing Exposure to exterior door closing / opening Person too close to moving train
Driver/staff related	Driver confused or distracted Driver incapacitated Driver fails to maintain proper lookout Cab ergonomics not optimized Potential for assault Person exposed to sudden train movement
Personal hazards	Driver or other staff member trip, slip or fall hazard entering Gap between train and platform Gap between train and walkway Potential for slip / trip / fall Potential for trap / cut hazard Potential for injury carrying out maintenance activities Potential for manual handling injury
Passenger related	Exposure to interior door closing/opening Person trapped in train doors Exposure to exterior door closing / opening Exterior door open whilst train moving Exterior door opens off platform / wrong side Person exposed to sudden train movement (acceleration/deceleration) Excessive pressure in train Person exposed to extreme temperature in train interior Lack of adequate ventilation in train Potential for assault Structural collapse of interior system / equipment

	Train overcrowded
Exposure to hazardous/energetic phenomena	Exposure to arcing Exposure to raised electrical potential Exposure to biological / toxic substances Exposure to corrosive / reactive substances Exposure to noise Exposure to vibration Exposure to surfaces / liquids at extreme temperatures Exposure to pressurized system / explosion Exposure to fire / smoke Exposure to contaminated food or water
Related to train movement	Train hit by flying object Train colliding with obstacle Train colliding with other train Projectile originating from train movement Object on track Aerodynamic force created by train movement Rail vehicle falls/moves during maintenance Detraining hazard
Other technical hazards	Excessive electromagnetic emissions from system System has insufficient immunity from electromagnetic Train overloaded Pollution of environment
Authorisation of train movement	Train fails to stop at intended location Train moves in wrong direction Unauthorized train movement Train not detected by railway infrastructure Train overspeeds Failure of signaling (trackside/cabside)
Technical failures of rolling stock	Failure of train wheelset, bogie, or suspension Train unstable Unwarranted train division Train overspeeds Inadequate structural integrity of train
Technical failures of track/infrastructure	Defective track Uneven track/track level not maintained Insufficient ballast support Lack of vertical support

	Lack of transversal support Sun kink/Buckling[15] Track gauge not maintained Track loose from sleepers Breach of track or damage to track Switch point failure Infringement of gauge clearance Object or vehicle on track Train not detected by railway infrastructure Failure of catenary system Flooding
Emergency	Rail system functions cannot be correctly operated during emergencies Inadequate life-saving equipment provided Inadequate communication Person trapped inside train in an emergency

[15] Solkurver

Til vurdering af systemer/situationer, hvor der er overvejende risiko for ulykker for enkeltpersoner, er det muligt at anvende tjeklisten i Tabel 5. Den er baseret på en langvarig registrering af arbejdsulykker i Holland og Danmark, og disse oplysninger er bearbejdet med henblik på at kunne lave en risikoanalyse af arbejdsulykker (Jørgensen et al., 2010). Med hensyn til arbejdsulykker kan tjeklisten betragtes som værende udtømmende. Til brug for jernbaner kunne nogle emner være specificeret i større detaljer, fx "påkørsel af køretøj" skulle omfatte (forskellige typer af) rullende materiel.

Emnerne er præsenteret som den skadeforvoldende hændelse (ulykke). Registrerede konsekvenser er dødsfald, varige mén eller alvorlig skade (hospitalsindlæggelse). For følgende ulykker er sandsynlighed for dødsfald mindre end 0,2 % (dvs. for de øvrige er den større) (Jørgensen et al., 2010):

20. Ramt af faldende genstande - fra manuelle løft
27. Ramt af håndværktøj holdt af anden person
31. Støde imod/ind i genstande
32. Begravet under løst materiale
35. Ramt af eget håndværktøj
43. Forbrænding - forfrysning/forbrænding ved kolde/varme overflader eller åben ild
45. Udslip af skadelige kemikalier fra åbne beholdere
48. Frigørelse af kemiske risici fra lukkede beholdere - transport
49. Frigørelse af kemiske risici fra lukkede beholdere - lukning
51. Ekstreme kraftanstrengelser - tunge løft
52. Ekstreme kraftanstrengelser - uhensigtsmæssige bevægelser
55. Ildebrand - brandslukning

Tabel A 2 Tjekliste med farer for ulykker for enkeltpersoner (passagerer og ansatte i jernbaneselskaber). Listen er baseret på registrering af flere tusinde arbejdsulykker I Holland og Danmark. Ved anvendelse på passagerer skal ""arbejde" eller "arbejdes" hvor muligt erstattes med "færden" hhv. "færdes". På grund af baggrundsmaterialet må denne liste anses for at være udtømmende for denne type ulykker.

A. Det underlag, hvor der færdes eller arbejdes • Arbejde i højde • Arbejde på samme niveau	1. Fald fra højde – flytbare stiger 2. Fald fra højde – faste stiger 3. Fald fra højde - trappestiger 4. Fald fra højde - rebstiger 5. Fald fra højde – mobile stilladser 6. Fald fra højde - faste stilladser 7. Fald fra højde – op/nedtagning af stillads 8. Fald fra højde – tag 9. Fald fra højde – arealer, gulve med store niveauforskelle 10. Fald fra højde – faste platforme 11. Fald fra højde ned i hul (fx i jorden, gulv) 12. Fald fra højde – mobile platforme 13. Fald fra højde – holdende køretøj 14. Fald fra højde – arbejde i højde i øvrigt uden værn 15. Risiko for at snuble eller skrid i samme niveau 16. Fald fra trappe eller skrå flader

B. De omgivelser, der færdes eller arbejdes i. • Arbejde hvor genstande kan falde ned • Arbejde hvor genstande kan flyve rundt • Arbejde, hvor en person kan blive ramt af genstande, støde ind i noget eller blive klemt • Arbejde, hvor en person kan blive begravet • Arbejde med mennesker og/eller dyr	17. Ramt af faldende genstande - kran eller hejs 18. Ramt af faldende genstande - mekaniske løft (ekskl. kran) 19. Ramt af faldende genstande - fra transportmiddel eller -bånd 20. Ramt af faldende genstande - fra manuelle løft 21. Ramt af faldende genstande - øvrige genstande i højde 22. Ramt af flyvende genstande – fra maskiner eller håndværktøj 23. Ramt af flyvende genstande – fra genstande under tryk/pres 24. Ramt af flyvende genstande – som er blæst med vinden 25. Påkørsel af køretøj 26. Ramt af rullende/glidende genstande 27. Ramt af håndværktøj holdt af anden person 28. Ramt af genstande holdt af anden person 29. Ramt af svingende genstande 30. Blive klemt mellem genstande 31. Støde imod/ind i genstande 32. Begravet under løst materiale 33. Udsat for aggressive mennesker (vold) 34. Udsat for dyrenes adfærd (fald, bid, stik, spark)

C. Hvad der arbejdes med eller ved. • Arbejde med maskiner og værktøj • Arbejde med/på køretøjer • Arbejde med/nær elektricitet • Arbejde med/nær varme og/eller kulde • Arbejde med/nær kemikalier • Arbejde med tunge løft	35. Ramt af eget håndværktøj 36. Ramt af bevægende dele af maskine - betjening 37. Ramt af bevægende dele af maskine - vedligehold 38. Ramt af bevægende dele af maskine - klargøring 39. Ramt af bevægende dele af maskine - rengøring 40. Tab af kontrol over køretøj 41. Kontakt med elektricitet – elektrisk udstyr 42. Kontakt med elektricitet – ved installation/reparation 43 Forbrænding - forfrysning/forbrænding ved kolde/varme overfalder eller åben ild 44. Ildebrand - antændelse fra "varmt" arbejde 45. Udslip af farlige kemikalier fra åbne beholdere 46. Kontakt med utildækkede farlige kemikalier (uden udslip) 47. Frigørelse af kemiske risici fra lukkede beholdere - arbejde/fyldning/tapning 48. Frigørelse af kemiske risici fra lukkede beholdere – under transport 49. Frigørelse af kemiske risici fra lukkede beholdere – ved lukning af beholder 50. Frigørelse af kemiske risici fra lukkede beholdere - arbejde i nærhed af udslip 51. Ekstreme kraftanstrengelser - tunge løft 52. Ekstreme kraftanstrengelser - uhensigtsmæssige bevægelser

D. Omgivelser af særlig farlig karakter. • Arbejde med/nær højspænding • Arbejde med/nær brandfarlige materialer eller processer • Arbejde, hvor der er risiko for kvælning, mangel på ilt • Arbejde med/nær eksplosionsfarlige produkter eller processer	53. Kontakt med elektricitet – højspændingsledninger 54. Ildebrand - brandbare og letantændelige stoffer 55. Ildebrand - brandslukning 56. Kvælning/forgiftning - arbejde i lukkede rum 57. Kvælning/forgiftning - arbejde med åndedrætsværn 58. Drukning - arbejde i/under vand eller andre væsker 59. Drukning - arbejde over/i nærheden af vand 60. Fysisk eksplosion 61. Kemisk eksplosion – damp eller gas 62. Kemisk eksplosion - støv 63. Kemisk eksplosion – eksplosiver 64. Kemisk eksplosion – eksotermisk reaktion

CLC/TR 50126-2 (CENELEC, 2007) indeholder i dets bilag B en række eksempler på tjeklister og måder at ordne generelle lister med farer på. Den generiske tjekliste fra Bilag B.1 er vedlagt i nedenstående tabel. Listerne er ikke nødvendigvis udtømmende; det anbefales at sikre for hvert projekt, om listen er dækkende. Bemærk, at listen mangler farer i relation til funktionalitet og integritet af infrastruktur (fx styrke, sætninger, udmattelse). CLC/TR 50126-2 bilag B indeholder også farelister for naboer (tredjepart) , passagerer og jernbanepersonale.

Tabel A 3 Generiske tjeklister for diverse typer af systemer eller aspekter fra CLC/TR 50126-2 (CENELEC, 2007)

Functional aspects (related to functional specifications)	Alarms and warnings Indication of failure Interlocks Maintenance and support Point setting Signal aspects Velocity control Software malfunction Software crash Vehicle structure integrity Deceleration control Train doors operation Gauge infringement Vehicle separation (uncoupling) Train separation Level crossing Train/track interaction Emergency controls Train/Platform Obstacle on track Recovery from failure Slips and trips On train services and facilities Environmental influences

Mechanical (mechanical systems/equipment)	Corrosion Cryogenic fluids Derailment Exhaust gases Fire Foreign body and dust Insect, rodent or mould damage Lasers Overheating Pressure systems Shock and vibration Vandalism Ventilation Humidity Flooding
Construction (civil engineering)	Access hazards at site Site preparation hazards Construction hazards Environmental effects Vandalism Interference with normal railway operating procedures Training and control of contractors

Electrical (electrical systems, equipment	Electromagnetic interference Fire and explosion initiation Insulation failure Lightning strikes Loss of power Traction current Protection against earth faults Indirect and direct contact Emergency switching and isolation Overcurrent protection and effects of disconnection Current rating
Operation and support (operating and maintenance procedures)	Accessibility for maintenance Documentation Failure to activate on demand Human factors Inadvertent activation Lighting Manuals Spares Training Start-up Close-down Re-setting

Occupational health	Asbestos Asphyxiates CFC's Corrosive materials Cryogenic fluids Electrocution Exhaust gases Fire High temperature Injury from moving parts LASERs Noise and vibration Pressure systems Radioactive materials Toxicity Electrical overheating

Bilag B Oplysninger om jernbaneulykker

Følgende databaser indeholder oplysninger om jernbaneulykker med adgang til ulykkesrapporter eller sammenfatninger på engelsk:

- UK Rail Accident Investigation Branch (https://www.gov.uk/government/collections/catalogue-of-investigation-reports-and-bulletins
- Dutch Safety Board (http://www.onderzoeksraad.nl/en/sectoren/rail-traffic?filters%5Btype%5D=Afgeronde).

Det tyske jernbanesystem er det største (målt på tog-kilometer) i EU. Tyske ulykkesrapporter (kun på tysk) findes hos:

- Eisenbahn-Unfalluntersuchungsstelle des Bundes (http://www.eisenbahn-unfalluntersu-chung.de/SiteGlobals/Forms/Suche/EUB/DE/EUB_Untersuchungsberichte_StartFormular.html?nn=1075760)

Derudover er der også nogle internationale databaser med oplysninger om ulykker og (større) hændelser på engelsk eller tysk:

- European Railway Agency: ERAIL https://erail.era.europa.eu/ ulykkesindberetninger og sammenfatninger efter en fast skabelon på engelsk, fulde rapporter (hvis tilgængelige) kan være på nationalsprog. Det noteres, at sammenfatningerne ofte er mangelfulde (fx mangler beskrivelser af årsager "causation" ofte), der kan søges på årsager (causal factors)[16] og type af ulykke (occurrence);
- US National Transportation Safety Board: Railroad Accident Reports: http://www.ntsb.gov/investigations/AccidentReports/Pages/railroad.aspx, adgang til ulykkesrapporter på engelsk;
- Japan Transport Safety Board: Summaries of Major Railway Accident and Incident Reports http://www.mlit.go.jp/jtsb/railrep.html, adgang til sammenfatninger (inklusive sandsynlig årsag) på engelsk;
- Swiss Transportation Safety Investigation Board: Search for reports on events (marker "railway"): http://www.sust.admin.ch/en/dokumentation_bahnen_schiffe_berichte_ueber_ereignisse_suchen.html, (adgang til ulykkesrapporter på tysk, fransk eller italiensk);
- Transportation Safety Board of Canada: Rail investigation reports: http://www.bst-tsb.gc.ca/eng/rapports-reports/rail/index.asp, (adgang til ulykkesrapporter på engelsk og fransk);
- Australian Transport Safety Bureau, Rail safety investigations & reports: https://www.atsb.gov.au/publications/safety-investigation-reports.aspx?mode=Rail , (adgang til hændelsesrapporter på engelsk).

[16] I den udstrækning disse er rapporteret

This report presents guidance on structured hazard identification (HAZID) methods that can be used during risk assessment in the railway sector as required by the European Commission's Regulation on the common safety method for risk evaluation and assessment (CSM-RA). It provides guidance on methods and on how to use these methods so that railway undertakers and infrastructure managers are able to identify all reasonably foreseeable hazards that may exist in connection to the system changes being proposed. The demonstration of the proper use of such structured methods should provide confidence that all those hazards are identified. This guidance discusses the scope of hazard identification in the framework of CSM-RA, best practice in using workshops for hazard identification, and it presents four different structured methods: HAZOP and FMEA the use of check lists, and reusing hazard identifications from earlier, similar projects. The guidance concludes with discussing the application of HAZID methods on organizational and operational changes.

DTU Management Engineering
Institut for Systemer, Produktion og Ledelse
Danmarks Tekniske Universitet

Produktionstorvet
Bygning 424
2800 Lyngby
Tlf. 45 25 48 00
Fax 45 93 34 35

www.man.dtu.dk